Mutual Evaluation Report of the Republic of Kazakhstan

2023

ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism

CONTENTS

EXECUTIVE SUMMARY

1. This Report summarizes the AML/CFT measures in place in the Republic of Kazakhstan as at the date of the on-site visit of the EAG assessment team (September 12 – 30, 2022). It analyzes the level of compliance with the FATF Recommendations and the level of effectiveness of the AML/CFT system of the Republic of Kazakhstan, and recommends how the national AML/CFT system could be strengthened.

Key Findings

1. The Republic of Kazakhstan makes considerable efforts to identify, understand and assess the national ML/TF risks and develop measures to mitigate them. Despite the fact that the ML NRA has no finding on the specific ML risks, the approach used to assess the predicate offences that generate main proceeds and review ML-related criminal cases reflects the needs of the country. In turn, the TF/PF NRA clearly specifies inherent TF risks.

2. The national AML/CFT policy is shaped on an ongoing basis and is properly aimed at mitigating the identified ML/TF risks. The findings of the risk assessments were adequately taken into account to identify the tasks and measures to be accomplished and taken by competent authorities.

3. The findings of risk assessments are communicated to FIs, DNFBPs, VASPs and SRBOs through institutional and operational mechanisms.

4. There is scope to further improve the methodology of ML risk assessment, enhance understanding of inherent risks and use the NRA findings to develop comprehensive interagency plans to mitigate the identified risks.

5. A wide range of financial and other information is available to all LEAs/SSAs. LEAs/SSAs regularly and effectively request, receive (including proactively) and use the FIU financial investigation data and other relevant information to gather evidence for investigating money laundering, terrorist financing and predicate offences and tracing criminal proceeds.

6. The FIU is a core element of the national AML/CFT regime in Kazakhstan and has a vast amount of data at its disposal. The FIU uses modern technology and a high level of process automation to prioritize, initiate and assist in investigations of cases conducted by LEAs/SSAs.

7. The powers of pre-trial investigative authorities to detect, suppress and investigate ML crimes are implemented in accordance with the legislation of the Republic of Kazakhstan and taking into account the specific anti-crime tasks performed by each agency within its purview. In general, this work is carried out in a systematic manner.

8. The "follow the money" principle is consistently implemented in the country, measures have been taken to improve the methodology of parallel financial investigations, access to a wide range of necessary financial information is provided. The level of interagency cooperation is high. International cooperation is used for the purpose of combating crime in general and ML in particular.

9. The detected, investigated and prosecuted ML types are generally consistent with the nature of national threats and risks and national AML policy.

10. Natural persons convicted of ML offences are subject to proportionate, dissuasive and effective sanctions. No sanctions have been imposed on legal persons for ML in the country. If it is not possible to secure a conviction for ML, a criminal prosecution for the predicate offence is carried out. In cases prescribed by law, the institution of non-conviction-based (pre-trial) confiscation is applied.

11. Confiscation of property obtained by criminal means or acquired with criminally obtained funds and instrumentalities of crime, compensation for property damage caused by crimes is a priority task and means of implementation of the state criminal policy in the anti-crime sphere.

12. Confiscation takes place as part of the criminal prosecution of a person, and in cases provided for by law without a conviction, and is a direct consequence of the commission of an offence. Confiscation of the proceeds of crime, property acquired by criminal means, instruments and instrumentalities of crime, and property of equivalent value is applied.

13. Measures have been taken to intensify LEA/SSAs' efforts to search for assets abroad and their return.

14. The work on the execution of court decisions in terms of confiscation of property and compensation for criminal damage is not in enough extent effective.

15. Confiscation of non-declared (falsely declared) cash in administrative proceedings is not applied at all, and in criminal proceedings it is sporadic. Customs authorities have significantly limited powers and access to information resources compared to LEAs/SSAs. In this regard, the disruption of cash couriers' activities through the application of confiscation is not effective.

16. The maintenance of statistics at certain stages of criminal proceedings, including detection, investigation and prosecution for ML, as well as confiscation and provisional measures, is not comprehensive.

17. The country's authorities are well aware of the TF risks and respond appropriately. Overall, the LEA's investigations into TF, as well as the country's response, are consistent with the findings of the NRA and the TF risk profile of Kazakhstan. While LEAs pay serious attention to threats of international terrorism, the threat of terrorist financing within the country is not excluded, which the competent authorities take into account in their activities.

18. Kazakhstan seeks to deprive terrorists, terrorist organisations and terrorist financiers of their assets and funds through a variety of methods. The country has a system of implementing TFS that allows for their application without delay. The lack of referrals for inclusion on the UNSCRs may be a disadvantage, given the large number of individuals on the national List.

19. Interagency cooperation between supervisory and law enforcement authorities has been built in the country, which generally allows, if necessary, to collect and verify information about the activities of NPOs and their possible involvement in TF in a timely manner, as well as to exchange it, including at the international level. At the same time, no cases of involvement of NPOs in TF-related activities were identified in the assessed period.

20. Kazakhstan has a unified legal framework in the field of combating PF and TF. The competent authorities have taken measures to include persons involved in the TF and PF in the relevant Lists and the private sector – to freeze assets without delay.

21. All obliged entities, except for commodity exchanges and lawyers, have good knowledge and understanding of their AML/CFT obligations and risks existing in the country, their sectors and institutions. The obliged entities have a good understanding of the ML risks, and at lesser extent FT risks.

22. In most obliged entities the internal control measures are based on the statutory requirements set out in the legislation. At the same time, certain obliged entities (this mostly concerns STBs and PSPs and insurance companies) demonstrated implementation of their own internal risk mitigation measures.

23. All obliged entities apply CDD measures to customers and their beneficial owners and verity data using open and commercial databases and information sources. Obliged entities apply targeted financial sanctions, deny transactions, refuse to establish and maintain business relationships, and freeze assets. At the same time, some non-banking FIs tend to rely on the internal controls exercised by the STBs when opening and maintaining a customer's bank account or conducting transactions. There are some shortcomings in identification of BOs and national PEPs in DNFBPs.

24. In general, the obliged entities are reasonably well aware of and fulfils their obligations to send STRs regarding proceeds of crime and, to a lesser extent, terrorist financing. The bulk of STRs are sent

by the STBs, that is in line with the risk profile of Kazakhstan. At the same time, some obliged entities (commodity exchanges and insurance brokers) did not send or sent relatively few STRs, that cannot be explained by their low risk profile alone and is indicative of a lack of understanding and compliance with the STR reporting obligation. Not all DNFBPs report a refusal to establish a business relationship.

25. FIs activity covered by the FATF standards requires to be licensed or registered in Kazakhstan for the purpose of AML/CFT compliance monitoring and supervision by supervisory authorities, and supervisory authorities conduct regular inspections to identify unlicensed or unregistered activities. With the exception of lawyers, notaries, legal advisors and real estate agents, all DNFBPs shall be registered as legal entities. Lawyers, notaries, legal advisors, audit firms, casinos and organisers of gambling industry shall be licensed. Jewelers, legal advisors, real estate agents shall notify FMA about commencement of activities as obliged entity.

26. Supervisors effectively identify cases of criminals owning significant shares in FIs as well as holding managerial positions, but do not identify persons affiliated with criminals. The DNFBP sector and VASPs outside AIFC has certain mechanisms in place to prevent criminals from entering the market, both at the moment of registration or licensing for a few sectors and at the moment of notification of FMA as an obliged entity. The AFSA registers and licenses AIFC members that are DNFBPs and VASPs, and identifies BOs and affiliates, and checks for criminal history, sanctions, etc.

27. ARDFM and NB have most effectively applied various tools of risk-based approach in supervising the compliance of FIs with AML/CFT requirements, including on-site inspections and unplanned inspections and remote supervision. The APDC applied risk-based supervision to a lesser extent. FMA, MCS, IPAC, MoJ apply elements of risk-based supervision.

28. Supervisory authorities generally apply to FIs a wide range of corrective measures when complying with AML/CFT requirements. Nevertheless, these measures are not proportionate to the violations committed and not sufficiently effective to prevent subsequent violations of AML/CFT legislation by other obliged entities. Corrective measures in relation to DNFBPs are not diverse, and sanctions are not proportionate and dissuasive. AFSA applies various corrective measures, including to AIFC obliged entities' officials.

29. Information on the types of legal persons and the specifics and procedures for their establishment is public and available in Kazakhstan.

30. The competent and other authorities of Kazakhstan have generally demonstrated certain understanding of the vulnerabilities of legal persons, limited to examples of criminal prosecutions for predicate offences without in-depth analysis and involvement of all relevant authorities and the private sector. The risk of illegal use of legal persons for ML purposes is high. No cases of misuse of legal persons for TF purposes were identified at the time of the on-site mission.

31. In order to mitigate the risks of misuse of legal persons, a number of tools have been developed and implemented in the country. These include risk-based controls carried out by the SRC, but related only to tax administration and the prevention of the involvement of legal persons in predicate offences.

32. Several types of sanctions are applied to legal entities, including corrective measures, administrative fines, blocking of bank accounts, collection requests for tax arrears, imposition of fines and penalties. Penalties for failure to provide information are generally not applied. Several types of sanctions are applied to legal entities, including corrective measures, administrative fines, blocking of bank deposit accounts, collection requests for tax arrears, imposition of fines and penalties. Penalties for failure to provide information are generally not applied.

33. The State Database "Legal Persons" (SDLP) contains basic information on legal entities and information on beneficial owners of legal entities – residents of the Republic of Kazakhstan. The SDLP is public, however, the information related to BOs is only available to law enforcement and special and supervisory authorities, FMA and STBs. The source of BOs data is the information provided by

applicants during the registration of legal entities. Provided BO information is not verified by the registration authority for accuracy and relevance. FMA maintains its own register of BOs of legal entities, which unites data from several sources, such as the SDLP, AIFC register, securities depository, as well as the results of tactical analysis and materials of interaction with law enforcement agencies on relevant investigations. The FMA's register is available to law enforcement and special agencies and can also be used to initiate data changes in the SDLP.

34. Non-resident legal entities' BOs are identified by the FI or DNFBP at the time of accepting services by collecting and examining data from available public or commercial databases. Data on BOs of non-resident AIFC members are identified and verified quite effectively. The relevant information is provided to the competent authorities upon request.

35. The law does not stipulate activities of legal arrangements on the territory of the Republic of Kazakhstan. However, the AIFC developed regulatory documents on trusts. At the time of the on-site visit, no trusts were registered with the AIFC. The AIFC has developed no legal basis for activities of other types of legal arrangements.

36. International cooperation, including mutual legal assistance, is generally carried out in a constructive and timely manner. The GPO, as a central body (along with the SC) coordinates this activity, ensures recording of requests and their timely execution. Secure electronic communication channels are used for their transmission. However, feedback on the usefulness of the information provided within the framework of MLA execution is not requested on a systematic basis.

37. In the vast majority of cases, all competent authorities resort to MLA mechanisms when there is evidence of the transnational nature of the offence. Statistical information shows that competent authorities are confident in resorting to MLA mechanisms and that, in general, the assistance requested corresponds to the country's risk profile.

38. LEAs/SSAs have been successful in identifying, seizing and confiscating assets abroad.

39. The authorities of the Republic of Kazakhstan generally cooperate effectively in the field of extradition and most of the relevant incoming requests are granted.

40. LEAs/SSAs and FIU effectively cooperate and exchange information in other forms at various international venues. Such cooperation leads to concrete practical results.

41. International cooperation of FI supervisors is based on international agreements and there are no regulatory obstacles to the exchange of relevant information.

42. All competent authorities are able to receive and transmit beneficial ownership information through MLA and other forms of international cooperation.

Risks and General Situation

2. The Republic of Kazakhstan is taking significant efforts to identify, understand and assess its ML/TF risks and develop measures to minimize them.

3. The first national ML/TF risk assessment was conducted in the country in 2018 and was of a closed nature. Since 2018 AML/CFT system of Kazakhstan have overcame the significant changes. In 2021, two separate NRA were conducted – in respect of ML and in respect of FT/PF; all competent authorities and the private sector were involved in them. For this purpose, own methodology has been developed based on the OSCE Guidance on the collection of data to conduct the ML/TF risk assessment and Words Bank's Risk Assessment Tool. The summary of the both NRA was published on FMA's official web-site and on government authorities' web-sites. It can be concluded that the country has revised the results of the previous assessment and carried out some reforms aimed at minimizing the identified AML / CFT risks and improving the efficiency of financial intelligence, supervisory and law enforcement agencies.

4. The ML NRA identifies tax crimes, illegal business activities, corruption, embezzlement of public funds, fraud and illicit drug trafficking as the offences posing high threat.

5. The main predicate offences for money laundering are: issuance of "fictitious" (fake) invoices; misappropriation or embezzlement of entrusted third party's property; illegal gambling operation; illicit trade in crude oil and petroleum products; tax evasion; fraud; breach of excisable goods marking procedure; production, storage or sale of counterfeit money; and infliction of pecuniary loss by deception.

6. The consolidated CFT efforts taken by the authorities have led to significant improvement of the criminal environment since 2017, and, at present, the TF risks could be assessed a medium. The assessors considered the level of coordination and effectiveness of actions taken by the competent authorities to detect and disrupt TF activities, consistency of the undertaken CFT efforts with the risks, vulnerabilities and threats identified in the NRA, and cooperation of the competent authorities with the FIU in the fight against terrorist financing.

7. No terrorist acts were committed in Kazakhstan in 2017-2021.

Overall Level of Effectiveness and Technical Compliance

8. The Republic of Kazakhstan has made significant progress in building an effective AML/CFT/PF system. As part of the ongoing reforms in the state, significant changes have been made to the AML / CFT / PF legislation, coordination and interaction mechanisms have been improved, the working mechanisms of FIs and DNFBPs have been improved, a significant number of automated systems have been introduced to ensure the efficiency of the activities of all participants in the system.

9. Kazakhstan has made significant improvements in its overall level of technical compliance with the FATF Recommendations, although some shortcomings remain. The legislation of the Republic complies or substantially complies with most of the requirements of the FATF Recommendations. Since the previous mutual evaluation, most of the legal acts and other legislative acts related to the issues under consideration have undergone significant changes. The legislation governing the powers of the LEA and the competence of the FIU is in line with AML/CFT/CPF standards. ML and TF crimes have been criminalized, mechanisms for freezing and confiscation of assets have been established, which, however, need to be improved. The powers of the competent authorities for coordination and interaction in the field of AML/CFT/CPF both at the national and international levels have been regulated. Measures for the application of CDD, storage of data and submission of STRs by reporting organizations are legislatively fixed.

10. The Republic of Kazakhstan has achieved a substantial level of effectiveness in terms of identifying, understanding and minimizing risks, as well as coordination and interaction. Also at a significant level is the activity of the FIU and the use of operational financial information for the purpose of detecting, investigating and suppressing, as well as adjudicating ML/TF crimes and predicate offences. The country has built an effective CFT system based on preventive measures and the timely application of the TFS mechanism. Some progress has been made in applying proportionate and targeted measures to the activities of NPOs vulnerable to exploitation for TF purposes. Improvements are required in terms of MLA, transparency of legal persons and arrangements, and confiscation issues.

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

11. The Republic of Kazakhstan used its own methodology to assess ML and FT/PF risks. All competent authorities and the private sector were involved in the preparation of the NRA. To prepare the NRA, a large volume of quantitative and qualitative data was used.

12. The approach used in ML NRA, which enables to assess predicate offences that generate main proceeds and review ML-related criminal cases, highlights the national priorities, but does not contain a conclusion on specific ML risks.

13. The TF/PF NRA clearly highlights the FT risks of the country. The evaluators agree with the findings

of the FT/PF NRA on the average risk level, taking into account a number of factors and measures that national competent authorities apply to mitigate the identified risks.

14. In the course of the NRA, the risk assessments of the use of virtual assets and the NPO sector was also conducted; in addition, assessment of the vulnerabilities of legal entities was conducted. However, the NRA does not assess the national cross-border ML risks. Despite this fact, competent authorities and the private sector have demonstrated that they understand the cross-border risks related to cash flow.

15. The national AML/CFT policy is appropriately aimed at taking measures to mitigate the identified ML/TF risks. Kazakhstan implements an ongoing and coordinated process to develop policy based on the outcomes of official risk assessments. Appropriate national strategies and action plans developed, inter alia, based on the 2018 and 2021 ML/TF national risk assessments, are an integral part of the strategic and operational national policy to combat ML/TF in the country.

16. National interaction and cooperation are the strengths of the Kazakh AML/CFT framework. FMA is responsible for coordination of legislative and operational AML/CFT activities and receives a high-level support from the country's leadership. Kazakhstan has various interagency coordination mechanisms.

17. The NRA outcomes are adequately communicated to the private sector through both institutional and operational mechanisms. FIs, DNFBPs and other sectors that should follow the AML/CFT requirements were directly involved in national and sectoral risk assessments.

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

18. All LEAs/SSAs regularly and effectively obtain and use financial intelligence and other relevant information to gather evidence for investigations of money laundering, terrorist financing and predicate offences and tracing criminal proceeds. Information may be obtained either independently or through the FIU.

19. The FIU has a vast amount of data at its disposal, including a large number of suspicious transaction reports and reports of transactions subject to mandatory monitoring. The FIU uses state-of-the-art technology and a high level of process automation to prioritize, initiate and facilitate investigations conducted by LEAs/SSAs.

20. The information contained in the FIU database is used to assist ongoing investigations, as well as to initiate new investigations into predicate offences and, less frequently, money laundering (except the EIS) and terrorist financing. Case studies and statistics show that analysis data are used to investigate cases that are proactively referred to law enforcement authorities as well as to assist ongoing investigations.

21. LEAs/SSAs have also demonstrated that financial investigation data communicated proactively or upon request is of high quality and an inseparable part of their work.

22. Most threshold and suspicious transaction reports are received by the FIU from financial institutions; DNFBPs submit them in smaller numbers. The FIU also receives other additional information from STBs upon request. Besides that, the FMA also receives information on transactions suspended by the obliged entities prior to their conduct due to suspicion of ML/TF.

23. The FIU has excellent resources and information capabilities and competent analysts who have in-depth knowledge of the national AML/CFT system specificities.

24. AML/CFT cooperation at the national level is a strength of the Kazakh AML/CFT system. LEAs/SSAs noted the close cooperation and effective coordination on ML/TF issues, for which purpose separate dedicated platforms were established to determine the directions of state policy in this area. The exchange of information between the FMA and the RK competent authorities is carried out exclusively via secure communication channels.

25. In the Republic of Kazakhstan the activity on detection, suppression and disclosure of ML crimes is carried out in the form of a criminal intelligence activity and pre-trial investigation. The powers of pre-trial authorities are performed in accordance with the legislation and taking into account the specific tasks in the

field of combating crime, carried out by each agency within its competence. In general, this work is conducted in a systematic manner.

26. Since 2017, there has been a downward trend in the number of registered predicate crimes, which in turn affects the number of detected cases of ML. The majority of ML crimes are committed by self-laundering. Failure to establish elements of the predicate crime when detecting the fact of ML does not prevent pre-trial investigation on legalization. Initiative reports of suspicious transactions by FIUs are also grounds for launching a pre-trial investigation into money laundering.

27. The Republic of Kazakhstan consistently implements the "follow the money" principle. For the purposes of conducting parallel financial investigations and exercising other powers the LEAs/SSAs have access to a wide range of information about individuals and legal entities, including financial information; a number of LEAs have established special units, whose competence includes exclusively conducting parallel financial investigations.

28. The competent authorities have the necessary human, informational and analytical resources, continuous professional development of employees is carried out.

29. The level of interagency cooperation is high. International cooperation is used for the purposes of combating crime in general and ML in particular.

30. The types of ML detected, investigated and prosecuted generally correspond to the nature of national threats and risks, as well as the national policy in the field of AML. The state pursues a policy of combating shadow economy, corruption, offences in the sphere of economic activity, tax and customs offences, and illicit trafficking in narcotic drugs and psychotropic substances.

31. The Republic of Kazakhstan prosecutes various types of ML, there are no aspects of the investigative, prosecutorial or judicial process that prevent or delay the prosecution and application of sanctions for ML.

32. Individuals convicted of ML offences are subject to proportionate, dissuasive and effective sanctions. No sanctions have been imposed on legal persons for ML in the country.

33. If it is impossible to obtain a conviction for ML, criminal prosecution for the predicate offence is carried out, and if a conviction for ML cannot be secured due to search, death, amnesty of the person or expiry of the statute of limitations, the institution of pre-trial confiscation is applied.

34. Confiscation of property obtained by criminal means or acquired by criminal means, instrumentalities and means of committing a crime, compensation for property damage caused by crimes is a priority task and one of the measures of implementation of the state criminal policy in the field of combating crime.

35. The confiscation of the proceeds of crime, property acquired with the proceeds of crime, instrumentalities and means of crime, and property of equivalent value is carried out as part of the criminal prosecution of a person, including in some cases without a conviction, and is a direct consequence of the commission of an offence.

36. The criminal prosecution authorities are exercising their procedural powers to enforce confiscation. Measures have been taken to intensify their efforts in the search for assets abroad and their return. Aspects hindering the application of confiscation include the lack of practical mechanisms for taking provisional measures in relation to VAs.

37. Confiscation of undeclared (misdeclared) cash in administrative proceedings is not applied at all, in criminal proceedings it is sporadic. The suppression of cash couriers through the application of confiscation in this regard is not effective, including due to the limitations of customs authorities in obtaining law enforcement information as compared to the LEAs/SSAs.

38. The statistics of the identification, investigation and prosecution of ML, as well as the application of provisional measures and confiscation are not comprehensive and require adjustment of approaches to its accumulation.

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

39. The country's authorities clearly understand the threat of international terrorism and the external and internal factors that contribute to the involvement of citizens in terrorist activities, among which the most relevant for Kazakhstan is the radicalization of the population through involvement in destructive religious movements and propaganda of terrorist ideas.

40. In Kazakhstan measures have been taken to coordinate the actions of all actors engaged in the fight against terrorism and to ensure a high level of cooperation among all government authorities and organizations.

41. TF detection and prosecution is one of the activities of LEAs/SSAs in the field of counter-terrorism. LEAs/SSAs have the necessary human, material and technical and information and analytical resources. Operational capabilities of the FIU are actively used for the purposes of identifying TF, and parallel financial investigations are conducted. National security authorities ensure the proper quality of the CIDA and pre-trial investigations into TF offences. The results of criminal prosecutions are consistent with the NRA findings and the country's risk profile.

42. The main authority responsible for detecting, suppressing and investigating terrorist offences, including TF, is the NSC. At the same time, the activities of other LEAs (EIS and MIA) engaged in combating terrorist offences should be intensified.

43. The sanctions applied by the courts to natural persons for TF offences are effective, they are dissuasive and generally proportionate, since they are imposed taking into account the public danger of the act and personal background. At the same time, the information provided did not allow to make a definitive conclusion about the nature of sanctions in relation to legal persons.

44. In general, Kazakhstan has built and uses a system that meets the requirements for the application of targeted financial sanctions without delay. Despite the introduction of amendments to the regulatory legal framework of the Republic of Kazakhstan in 2020 aimed at stipulating at the legislative level the mechanisms and procedures for the implementation of the TFS requirements by the obliged entities and individual government authorities, Kazakhstan has demonstrated that, before the adoption of these amendments, TFS were also applied without delay.

45. The majority of obliged entities understand their obligations with regard to the implementation of TFS measures.

46. Kazakhstan carries out certain work to control NPOs in order to prevent them from being misused for TF purposes without prejudice to their legitimate activities. The country provides for measures aimed at preventing registration of NPOs exposed to such risk, termination of their activities and liquidation, as well as applying sanctions for non-compliance of NPOs with the relevant control requirements of the country. At the same time, the work is generally based on the NRA and TF SRA findings in terms of the misuse of NPOs, according to which the average risk level is assigned to charitable and religious organizations.

47. NPOs sufficiently understand the vulnerability of organizations to the use for TF purposes, but do not fully have the mechanisms of their own actions in the event of such situations.

48. Kazakhstan has a unified legal framework in the field of combating PF and TF. In general, the country has built and uses a system that meets the requirements for the immediate application of targeted financial sanctions. In addition, an effective customs and export control system is in place, one of the tasks of which is the control of dual-use goods.

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

49. In the financial sector, most obliged entities have good enough understanding of AML/CFT obligations and risks existing in the country, sectors and their institutions. However, understanding of risks concerns primarily potential involvement in predicate offences, but not in ML/TF schemes (except for STBs, PSP and insurance companies). In general, the DNFBPs have a good understanding of level ML and

TF/PF threats and vulnerabilities in sectors. They also understand the level of national ML risks and, to a lesser extent, the level of national TF/PF risks. Sectoral ML/TF/PF risk assessments would allow to improve understanding of their own risk profiles. VASPs have a good understanding of ML and TF/PF risks and also risks related to misuse of digital assets for ML/TF/PF purposes.

50. FIs conduct CDD when establishing business relationships and perform ongoing monitoring of transactions carried out by customers and their beneficial owners, but the practice of applying standard, simplified and extended measures varies from sector to sector, as well as in individual obliged entities. The full range of CDD measures, depending on the risk level assigned to the client, is applied mainly in STBs, but to a lesser extent in other sectors. There are also shortcomings in identification of ultimate beneficial owners of corporate customers.

51. In general, DNFBPs and VASPs have demonstrated a significant level of understanding of the AML/CFT obligations in context of their sectoral specificities. The DNFBP and VASP sector entities implement internal controls and comply with the ICR requirements related to conducting customer due diligence and screening customers against the lists. Besides that, all DNFBPs and VASPs have demonstrated a good awareness of their TFS obligations and understanding of the need to apply targeted financial sanctions and to keep confidentiality. At the same time, there are shortcomings in identification of beneficial owners in context of transactions carried out by natural persons and also in identification of domestic PEPs, since these requirements have been implemented in the AML/CFT Law relatively recently. All demonstrated understanding and knowledge of the need to identify and report suspicious transactions/activities to FMA.

52. FIs apply enhanced CDD measures to high-risk customers, but certain FIs prefer to refuse to establish or continue business relationships with high-risk clients instead of taking enhanced CDD measures. Not all obliged entities identify and report suspicious transactions to the FMA, although this deficiency is observed in sectors exposed to a low risk where suspicious transactions are minimized.

53. The banking sector, which represents the largest and most significant sector of the financial system through which monetary transactions pass, is the most effective in applying preventive AML/CFT measures. The rest of the obliged entities tend to rely on the controls implemented by the STBs to conduct customer transactions.

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

54. Supervisory authorities regulate, control and monitor obliged entities' compliance with the AML/CFT legislation, as well as controls to prevent criminals from owning shares in obliged entities through licensing or registration of their activities, and through subsequent regular inspections, taking into account certain risk indicators of obliged entities' activities.

55. At the same time, supervisors understand risks as the involvement of FIs in the commission of predicate offenses, and accordingly, the quantitative and qualitative criteria for the FIs risk assessment used to conduct risk-based supervision are not based on ML/TF risks per se. Supervisors have not identified instances of the involvement of FIs in ML/TF schemes. Supervisors of DNFBPs are generally aware and understand the risks in the sectors they supervise, and take mitigation measures. However, the measures are mainly focused on prevention and are not related to addressing the preconditions for the identified ML/TF risks, with the exception of certain measures taken by the MCS.

56. Supervisors apply various tools of a risk-based approach in AML/CFT supervision in relation to FIs, but the ARDFM does not fully implement consolidated supervision of the international financial groups. The FMA, using the "Personal Account" online service on the FMA portal, checks the performance of the obliged entities on a daily basis and is able to respond promptly to AML/CFT deficiencies in their performance. The government authorities supervising DNFBPs have not shown much activity in using this service to detect/prevent AML/CFT breaches.

57. The application of sanctions and supervisory response measures are effective in most cases in

eliminating identified breaches and preventing their repeating in the same FIs, but have no effect in reducing the number of breaches of AML/CFT legal requirements in general.

58. Although the FMA does a great deal of work to clearly understand the AML/CFT obligations of the obliged entities, other supervisors are less active in this direction and rely more on the FMA and industry SRBs.

59. The AFSA uses a risk-based supervisory approach model developed on the basis of the classic risk management approach (inherent risks minus controls constitute residual risk), taking into account the inherent business characteristics of AIFC members based on the available individual risks of the obliged entities. Quantitative and qualitative criteria are taken into account in this model. At the time of the on-site mission, there were no inspections completed up to the date of identification and sanctioning of AIFC members.

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

60. Information on the types of legal persons and the specifics and procedures for their establishment is public and available. All legal persons created in the Republic of Kazakhstan are subject to state registration, and the AIFC members are registered by the Registrar of Companies of AFSA.

61. As the main risks, the authorities identified their use for illegal cash-out; their use in illegal activities of economic entities registered by foreign citizens; for the creation of financial pyramids; for evasion of taxes and other obligatory payments, primarily by issuing fictitious invoices; in online casino activities. In general, these risks correlate with those identified by the ML/TF NRA and the risks that are on the radar of the competent government authorities of the Republic of Kazakhstan.

62. A number of mechanisms have been developed and implemented to mitigate the risks of misuse of legal persons. These include controls carried out by the SRC based on a risk-based approach, but related only to tax administration and the prevention of the involvement of legal persons in predicate offences. However, sanctions are generally not applied for failure to report changes in basic (except for location) or BO information. Information on the involvement of legal and natural persons in illegal activities based on the materials of operative checks, criminal cases and analytical work is transmitted by the criminal prosecution authorities to the FMA. In order to inform the obliged entities, the list of such persons is posted on the FMA website. The AIFC has implemented risk assessment measures during the registration period of members, which are regularly updated, as necessary.

63. The competent authorities demonstrated, in general, good understanding of vulnerabilities of legal persons and the way they can be misused for criminal purposes. The supervisors demonstrated similar understanding and confirmed the NRA results in terms of vulnerabilities inherent in legal persons. Along with that, the typologies of misuse of legal persons for ML and predicate offences described in the Report on vulnerabilities do not seem to be fully developed, since they are based on individual examples of criminal prosecution without deep analysis and involvement of all interested authorities and the private sector. In this regard, the assessors conclude that the justification described in the Report on vulnerabilities for findings on the exposure of legal persons to ML and FT risks is not complete.

64. Being under the jurisdiction of the Ministry of Justice and integrated with 34 information systems of state authorities, the SDLP contains information about the name of the legal person, its place of registration, BIN, participation shares, head, individual identification number (further in this section – IIN), type of economic activity, form of incorporation, submitted by the applicant when registering information on the beneficial owner, etc., i.e. basic information about all legal persons registered in the country. The SDLP is a unified source of data on legal persons, that maintain interdepartmental electronic communication in the provision of public services and is used as necessary by the competent authorities. The SDLP is integrated with almost all interested state authorities which receive information automatically upon request. Information on the creation, types and characteristics of legal persons registered in AIFC is publicly available and posted on the website of the AFSA.

65. Since February 2022 this work has been methodologically streamlined and systematised in the form of a regularly updated automated module "Register of beneficial owners and persons likely controlling a legal person". Information from the FMA Register is available to competent authorities upon request. In case of discrepancies between the data in the Register and the SDLP, the FMA sends a notification to respective justice department with a request to arrange amendment of SDLP data by the legal person. The AIFC Registrar collects, cross-checks and maintains basic and BO information related to all residents of AIFC.

66. Non-resident legal entities' BOs are identified by the FI or DNFBP at the time of accepting services by collecting and examining data from available public or commercial databases. Data on BOs of non-resident AIFC members are identified and verified quite effectively.

67. The law does not stipulate activities of legal arrangements on the territory of the Republic of Kazakhstan. The AIFC developed regulatory documents on trusts. However, at the time of the on-site visit, no trusts were registered with the AIFC. The AIFC has developed no legal basis for activities of other types of legal arrangements. No foreign legal arrangements have been identified in the country.

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

68. International cooperation, including but not limited to provision of mutual legal assistance is generally performed constructively and in time. General Prosecutor's Office as the central authority and coordinator of such activities ensures that most of the queries are completed within the term of 3 months. At the same time, there are no standard procedures for registration of either incoming queries or the queries sent by the General Prosecutor's Office to other authorities. Besides, due to fragmented, non-systemic recording of query completion, the central authority is used to take little interest in the quality of the provided information, and requests feedback quite episodically, and fails to perform a proper analysis.

69. LEA/SSAs of the country successfully identify, arrest, and confiscate assets abroad thanks to, among other things, the Stolen Asset Recovery Initiative implemented in Kazakhstan in 2016. Alternative forms of international cooperation, including but not limited to CARIN, ARIN AP, ARIN-WCA, INTERPOL, and FOCAL POINT etc, are in use, but not all the law enforcement agencies demonstrated sufficient awareness of the possible benefits of such forms of international cooperation during the on-site mission.

70. The authorities of the Republic of Kazakhstan collaborate efficiently in the field of criminal extradition, and most of the corresponding incoming requests are executed.

71. Law enforcement agencies efficiently collaborate and share information at various international platforms in other forms. Such cooperation results in certain practical results.

72. International information exchange with FIUs is performed by the FMA systematically and together with a wide range of partners, and complies with the national risks of ML/TF.

73. International cooperation of the financial supervision authorities is based on international agreements, and there are no regulatory impediments to corresponding information exchange. The level of international cooperation in the field of supervision complies with the needs of regulators and the risks that may exist at this stage.

74. All the competent authorities can obtain and transfer information on beneficial owners through the MLA channels but not all the law enforcement and special authorities have a sufficient command of the corresponding procedures.

Priority Actions

The following is recommended to the Republic of Kazakhstan:

1. Analyse the reasons for the lack of successful prosecutions for ML without a predicate offence and take legislative measures where necessary. Intensify efforts to identify and suppress ML for corruption and drug trafficking offences.

2. Ensure the practical implementation of the administrative liability of legal persons for money laundering, expand the range of sanctions in relation to legal persons.

3. Consider amending legislation to expand the institution of pre-trial confiscation of criminal property, instrumentalities and means of crime in criminal cases.

4. Increase the effectiveness of customs authorities, and expand their powers, including by providing direct access to information resources of law enforcement and government authorities.

5. Ensure that confiscation is used as a measure of administrative responsibility for failure to declare (misdeclare) cash and that cases of administrative offenses in this category are the responsibility of the courts.

6. Take measures to ensure that all natural and legal persons (not only FIs, DNFBPs and VASPs) comply with the requirements of the TF and PF TFS.

7. Consider developing additional targeted measures in relation to NPOs vulnerable to the use for TF purposes, including in terms of ensuring control over the spending of funds by charitable and religious organizations, based on certain threats and risks of using NPOs for TF purposes.

8. Consider mechanisms of strengthening the ability of the obliged entities to identify companies owned or controlled by designated persons in order to identify possible cases of avoiding to comply with PF requirements.

9. When identifying BOs of legal persons, the obliged entities should identify BOs exercising effective control over the legal person and use available public or commercial databases.

10. Supervisory authorities should better understand the ML/TF/PF risks and risk-based supervision approaches, and conduct sectoral risk assessments.

11. It is recommended to correct administrative sanctions, including those applicable to the officials of FIs and DNFBPs violated the requirements of the AML/CFT regulation as well as expanding the range of corrective measures.

12. The registrators should take measures to arrange verification of information of BO of a legal person, submitted during registration, as well as to determine liability of applicants for providing unreliable information during registration (re-registration) of a legal person.

13. It is recommended to establish a regular exchange of information on BO accumulated by FMA, law enforcement agencies and the private sector when dealing with legal entities, with the registering authority to update the information on BOs in the SDLP.

14. The practice of applying proportionate and dissuasive sanctions should be introduced for legal entities and legal arrangements that do not provide registration authority with the changes in basic and BO information or provide it not in a timely manner.

15. The Republic of Kazakhstan should systematically request feedback, accumulate and analyze information about the usefulness of the information transmitted.

16. The Republic of Kazakhstan shall take steps to develop regulatory, organizational, and methodological mechanisms for execution of the requests related to criminal use of cryptocurrencies and other virtual assets (out of the AIFC) for money laundering.

17. Ensure quality collection and accumulation of 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	HP.9 TF investigation and prosecution	IO.10 TF preventive measures and financial sanctions	IO.11 PF financial sanctions
Substantial	**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**	**LC**

Preventive measures

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

R.21	R.22	R.23
C	**LC**	**LC**

Transparency and beneficial ownership of legal persons and arrangements

R.24	R.25
PC	LC

Powers and responsibilities of competent authorities and other institutional measures

R.26	R.27	R.28	R.29	R.30	R.31
PC	LC	PC	C	C	LC

R.32	R.33	R.34	R.35
LC	LC	LC	PC

International cooperation

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

MUTUAL EVALUATION REPORT

Preface

75. This report summarizes the AML/CFT/CPF measures in place in Kazakhstan as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the Kazakh national AML/CFT system, and recommends how the system could be strengthened.

76. This evaluation of the AML/CFT/CPF system was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by Kazakhstan in the technical compliance and effectiveness questionnaire, and information obtained by the assessment team during its on-site visit to the country on September 12-30, 2022.

77. The evaluation of Kazakhstan under the second round of the EAG Mutual Evaluations was conducted by an assessment team consisting of:

- Mrs. Anna Iglikova (Belarus);
- Mrs. Svetlana Poddubskaya (Belarus);
- Mr. Denis Kunev (Russia);
- Mr. Daniel Burda (Russia);
- Mr. Sardor Ikramov (Uzbekistan);
- Mrs. Natalia Radishevskaya (Luxemburg)
- Mr. Dzmitry Varabyou (EAG Secretariat);
- Mr. Mikhail Kolinchenko (EAG Secretariat);
- Mrs. Darya Kudryashova (EAG Secretariat);
- Mr. Soat Rasulov (EAG Secretariat).

78. The report was reviewed by: Shengnan Yan (China), Kostas Gkioulekas (Greece), Waleed Saeed Al Awadhi (United Arab Emirates) and the FATF Secretariat.

79. The previous mutual evaluation of Kazakhstan was conducted in 2011 using the 2004 FATF Methodology. The Mutual Evaluation Report of Kazakhstan was adopted by the 14th EAG Plenary in June 2011. The report is a public document accessible on the EAG website.[1]

80. Following the adoption of the first MER, Kazakhstan was placed in the EAG enhanced follow-up process. In November 2015, Kazakhstan presented the 3rd detailed follow-up report for its removal from the enhanced follow-up and placement in the regular follow-up process. Technical compliance with R.13 (Suspicious transaction reporting), R.35 (Conventions), SR.II (Criminalization of terrorist financing) and SR.IV (Suspicious transaction reporting) was considered as corresponding to the "largely compliant" (LC) level. However, review of progress made in respect of core R.1 (ML offence), R.5 (Customer due diligence) and key R.23 (Regulation, Supervision and Monitoring), SR.I (Implementation of UN instruments) and SR.III (Freezing and confiscating terrorist assets) did not allow for making a conclusion that Kazakhstan was compliant (C) or largely compliant (LC) with these Recommendations. Therefore, the Plenary requested Kazakhstan to present next enhanced follow-up report at the 24th EAG Plenary Meeting. Following the discussion of the report, the Plenary concluded that the country made a sufficient progress and removed Kazakhstan from the EAG enhanced monitoring process.[2]

[1] (eurasiangroup.org)
[2] 4th Follow-up Report - 2016.pdf (eurasiangroup.org)

CHAPTER 1. ML/TF RISKS AND CONTEXT

General Information

81. The Republic of Kazakhstan is a unitary, democratic, secular, legal and social state with a presidential form of government.

82. Kazakhstan gained independence on December 16, 1991. The capital of the country is Astana city. The Kazakh language is the official language. The Russian language is a language of interethnic communication.

83. Kazakhstan has a civil law system (also called Romano-Germanic legal system) which is based on binding rules and norms set out in the national legislative acts.

84. The legal system of Kazakhstan has a strict hierarchical structure where any lower-level law and/or regulation shall not contradict the higher-level laws and regulations. The Constitutions is the basic law of Kazakhstan. The current version of the Constitution of the Republic of Kazakhstan was adopted at a nationwide referendum on August 30, 1995.

85. The President of the Republic of Kazakhstan is the head of the state and the highest public official who determines the core principles of domestic and foreign policies and represents Kazakhstan domestically and in the international arena.

86. The executive power is exercised by the Government that presides over the system of executive bodies and supervises their activity.

87. The legislative power is exercised by the Parliament that consists of two chambers acting on a permanent basis, the Senate and the Majilis. The Senate (the upper chamber) is composed of elected members: two from each region and three cities of "state significance", including the capital city. Another fifteen members of the Senate are appointed by the President of Kazakhstan with a view to ensuring representation of all diverse national and cultural components of the society.

88. The Majilis (the lower chamber) is composed of one hundred and seven members, nine of whom are elected by the Assembly of People of Kazakhstan. Administratively, Kazakhstan is divided into 17 regions and 3 cities having the "state significance" status.

89. Kazakhstan has a population of over 19 million people.

90. With an area of 2,700,900 square kilometers, Kazakhstan is the ninth-largest country in the world. Kazakhstan shares borders of 7,591 kilometers with Russia to the north and west (the longest continuous land border in the world); 1,783 kilometers with China to the east; and 1,242 kilometers with Kyrgyzstan, 2,351 kilometers with Uzbekistan, and 426 kilometers with Turkmenistan to the south. Total length of the land border is 13, 200 kilometers.

91. The national currency of the Republic of Kazakhstan is tenge (KZT) which was introduced on November 15, 1993. The National Bank of the Republic of Kazakhstan is the only issuer of the national currency in the territory of Kazakhstan.

92. In 2021, the gross domestic product (GDP) of Kazakhstan amounted to USD 190.814 billion, while the GDP per capita stood at USD 10,041.5.

93. The Republic of Kazakhstan is a member state of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) since 2004.

1.1. ML/TF Risks an Scoping Higher Risk Issues

1.1.1. Overview of ML/TF risks

94. Kazakhstan's exposure to money laundering risks is primarily as a source of proceeds of crime.

Kazakhstan is not a major international financial center, nor is it a major hub for company formation or corporate services. However, operating is Kazakhstan is Astana International Financial Center (AIFC) located in the capital city. This is the territory with a special legal and regulatory regime for financial services established by the Constitutional Law on Astana International Financial Center. However, the country faces significant money laundering risks as a result of proceeds of crimes committed in Kazakhstan, including those related to historically high level of tax evasion and corruption, and its role of both a transit and destination country for narcotics trafficking.

95. Kazakhstan is a member of the Eurasian Customs Union which operates through supranational institutions. The customs controls are applied only at the external borders of the Union and, therefore, Kazakhstan has to implement special measures to combat cross-border movement of criminal money within the Union and suppress illicit trafficking of narcotic drugs. Cash is moderately used in Kazakhstan. Besides that, since funds obtained through crime may be converted into high-value assets, this gives rise to higher risks in certain sectors. The widespread use of cash may be exploited for ML/TF through the banking sector as well as through the money or value transfer services (MVTS) sector where payments are typically made in cash outside the existing business relationships.

96. Kazakhstan acts as a connecting link between the large and rapidly growing Chinese and Southeast Asian markets, on one hand, and the Russian and Western European markets, on the other hand, by providing road, railway and maritime (across the Caspian Sea) traffic, which makes it a potential transit point for movement of money and goods.

97. In view of its geographic location, Kazakhstan also faces threats posed by international terrorist organizations (such as ISIL) and activities of foreign terrorist fighters (FTFs). Nevertheless, the number of detected and prosecuted TF cases tends to decline in recent years and the share of TF offences in total number of terrorism-related crime is relatively low. Kazakhstan shows its readiness to contribute to strengthening the borders and preventing the penetration of radical Islamist cells in Central Asia through cooperation within the CSTO, RATS SCO, ATC CIS, etc. The Kazakh special services also pay attention to the Taliban's intention to eliminate terrorist cells of Central Asian origin in Afghanistan, as well as their desire to prevent the spread of the "Islamic State" in the region. In addition, the dynamics of detection and prosecution of TF are declining, and the share of these crimes in the overall structure of terrorist crimes is low.

1.1.2. National risk assessment

98. The first national assessment of ML/TF risks was conducted in Kazakhstan in 2018 and the findings of this assessment were classified. Since 2018, AML/CFT regime in Kazakhstan has experienced significant changes. In 2021, Kazakhstan conducted two national assessments of ML risks and TF/PF risks, respectively. These NRA reports are also classified, but there are also unclassified versions of these reports that are publicly accessible. It can be concluded that the country has reviewed and revised the findings of the previous assessment and implemented certain reforms aimed at mitigating the identified ML/TF risks and improving the effectiveness of operation of the FIU, supervisory and law enforcement authorities.

1.1.3. Scoping higher risk issues

99. The ML NRA identifies tax crimes, illegal business activities, corruption, embezzlement of public funds, fraud and illicit drug trafficking as the offences posing high threat.

100. The main predicate offences for money laundering (CC, Art. 218) are: issuance of “fictitious” (fake) invoices (CC, Art.216); misappropriation or embezzlement of entrusted third party’s property (CC, Art.189); illegal gambling operation (CC, Art.307); illicit trade in crude oil and petroleum products (CC, Art.197); tax evasion (CC, Art. 245); fraud (CC, Art.190); breach of excisable goods marking procedure (CC, Art.233); production, storage or sale of counterfeit money (CC, Art.231); and infliction of pecuniary loss by deception (CC, Art.195). These main types of predicate offences caused losses amounting to over KZT 2 billion, of which KZT 1 billion losses were inflicted by just the fraud-related offences. A total of 160 criminal offences covered by CC Article 218 (money laundering) were recorded in the assessed period

(although the number of this type of offences tends to decline - 79 ML offences in 2018; 42 ML offences in 2019; and 39 ML offences in 2020, 56 in 2021 г., 43 for 9 mths. 2022 г) which caused losses totaling KZT 128.7 billion.

101. The assessors thoroughly reviewed ML NRAs, as well as information from reliable third party sources (such as reports of other international organizations) in order to identify issues for enhanced focus in the course of this mutual evaluation. The issues identified were the following:

102. **Organized crime**. The criminal environment in Kazakhstan is characterized by the presence of organized criminal groups (OCGs) with international links, in particular with foreign crime syndicates from the former USSR Republics. Some of these groups are large, and generate profit from an array of criminal activity, particularly drug trafficking. These criminal proceeds are further used for supporting the operation of criminal business enterprises as well as for acquiring firearms, real estate property and luxury cars. Large amounts of criminal proceeds of OCGs are laundered abroad.

103. The assessment team considered the actions taken by authorities to investigate ML committed by organized criminal groups and their ability to confiscate proceeds and instrumentalities of crime when pursuing domestic ML cases with transnational elements. The assessors also considered measures taken by the FIU, law enforcement and supervisory authorities to disrupt these groups and their activities.

104. **Illicit drug trafficking**. According to the ML NRA, drug trafficking is one of the main predicate offences for ML and is one of the crimes generating the most revenue. A serious aggravating factor is the extensive cultivation of marihuana in the Chuy Valley, from which herbal (plant-based) narcotic drugs are supplied to other regions of Kazakhstan. Geographically, Kazakhstan is located on the so-called Northern Route along which heroin is supplied into Russia and other CIS and EU countries. According to the CIS Executive Committee, the largest average annual quantity of heroin (391 kilograms) was seized in Kazakhstan in 2016 - 2019.

105. Statistics indicate a slight increase in crimes related to drug trafficking in Kazakhstan. Between 2017 and 2021, 1,498 drug crimes (2017-2941, 2018-2076, 2019-1989, 2020-2144, 2021-2348), 7098 distribution (2017-1986, 2018-1218, 2019-1200, 2020-1301, 2021-1393) and 2154 illegal possession (2017-649, 2018-389, 2019-363, 2020-342, 2021-411) were reported. More than 112 tons of drugs were seized from illicit trafficking, including 127 kg. "heroin," more than 72 tons. "marijuana," 2.5 tons. 2.5 tons of "hashish" and more than 330 kg of synthetic drugs. 1,369 facts (2017-258, 2018-208, 2019-219, 2020-277, 2021-233, 7 months 2022-174) of illegal cultivation of drug plants were detected.

106. The assessment team considered the actions taken by the authorities to investigate the laundering of drug trafficking proceeds and their ability to identify and recover such proceeds laundered abroad.

107. **Corruption and embezzlement of public funds**. The ML NRA identifies corruption and embezzlement of public funds as generating significant criminal assets. Despite the extensive anti-corruption initiatives taken by the authorities, corruption remains a significant proceeds-generating crime. The Kazakh authorities recorded 103.2 thousand embezzlement-related offences that caused damages and losses amounting to KZT 1.8 trillion (KZT 17.4 million per crime, on average). In order to launder proceeds of this type of criminal activity, offenders use shell (fake) companies through which they cash out or transfer their ill-gotten money abroad. Besides that, such shell companies are used for investing the embezzled public funds into the shadow economy inflicting heavy losses on the state that allocates huge amount of funds from the national budget for financing the government-supported programs and national projects related to development of the national economy, improvement of the public health and education systems, increase of public employment, strengthening social stability and construction of socially important facilities.

108. The assessment team considered how authorities identify, investigate and prosecute the laundering of the proceeds of corruption—particularly relating to PEPs—and the authorities' activities to identify and recover these assets wherever located.

109. **Other types of predicate offences**. The assessors focused on analysis of actions taken by the law enforcement and special government authorities to identify crimes involving the laundering of proceeds of predicate offences posing high threat. Increased attention was paid to investigation if such criminal offences, including parallel financial investigations. The assessors also considered how other types of ML-related offences, i.e. self-laundering and third-party ML, are investigated by the authorities.

110. **Use of cash and shadow economy**. The distribution of cash is used moderately in the Republic of Kazakhstan. Besides that, since funds obtained through crime may be converted into high-value assets, this gives rise to higher risks in certain sectors. The widespread use of cash may be used for ML/TF through the banking sector as well as through the money or value transfer services (MVTS) sector where payments are typically made in cash outside the existing business relationships. The assessors considered the mechanisms deployed by the Kazakh authorities to mitigate the risk of ML using cash, including cross-border transportation of currency, as well as on remittances and the use of cash in real estate transaction and for purchasing precious metal and stones and other luxury goods.

111. **Misuse of DNFBPs for ML/TF**. According to the national legislation, the gambling activities are permitted only in specially designated areas (Burabai town in Akmola region and Kapchagai city in Almaty region). Although casinos are the obliged entities (subject to financial monitoring), they submit small number of STRs, despite the fact that the ML NRA and other sources indicate that casinos are used by criminals for illegal purposes. Risks in the DPMS sector are also high due, inter alia, to the presence of clandestine factories with counterfeit stamps, resulting in illegal products on the market, thefts from gold mines and factories. Real estate agents do not submit STRs, which may indicate either imperfection of the AML/CFT legal framework in this sector, or reluctance of real estate agents to comply with the statutory requirements in the area concerned, relying on the measures taken by notaries. The assessors considered how the authorities prevent criminals from penetrating the DNFBP sector or misusing the obliged entities for illegal purposes, and also how the obliged entities apply preventive measure, including CDD, record keeping and suspicious transaction reporting.

112. **Use of the second-tier banks and microfinance organizations in ML schemes**. Although the banking sector is the most regulated one in Kazakhstan, certain high-risk transactions potentially related to ML may still be carried out through this sector, including where large amounts of funds are transferred abroad and subsequently cashed out from accounts of straw men. Microfinance organizations represent a rapidly developing sector that is still featured by a large number of violations of the AML/CFT legislation, including failure to conduct adequate financial monitoring. The assessors focused on measures taken to identify ML schemes involving misuse of the second-tier banks and microfinance organizations and also on supervisory measures aimed at mitigating the risks of potential abuse of the second-tier banks, microfinance organizations and other financial institutions for ML purposes.

113. **Use of virtual assets in ML/TF schemes**. Kazakhstan has assessed the exposure of the VASP sector to potential abuse and involvement in ML/TF schemes. The ML/TF prevention and mitigation measures taken by the authorities are aimed at amending the legislation, monitoring and identifying prohibited Internet content and informing the obliged entities (that are subject to financial monitoring) about identified typologies. In Kazakhstan, virtual assets are legitimately used only by the AIFC member companies, all of which are obliged entities that are subject to financial monitoring. Most of them operate since 2019-2020 and, therefore, their customer base is too small or insufficient for conducting a comprehensive ML/TF risk assessment. At the same time, popular cryptocurrencies widely used in the global market may be used for committing predicate offences (e.g. payments for narcotic drugs, firearms, etc.) and for subsequent laundering of criminal proceeds. The assessors focused on actions taken by the FIU and the law enforcement and supervisory authorities to detect and suppress illegal use of virtual assets in the territory of Kazakhstan.

114. **Abuse/ misuse of legal persons and legal arrangements**. Kazakhstan has assessed risks of misuse of legal persons and arrangements for ML/TF purposes (the risk assessment report was adopted in May 2022). However, in the assessors' opinion, this risk assessment was not comprehensive enough and focused, to a large extent, on description of different types of legal persons, legal arrangements and non-profit

organizations and their registration/ licensing procedures. Besides that, illegal business activities and use of shell legal entities in ML schemes pose high threat. Therefore, the assessors thoroughly considered measures taken by the authorities to enhance transparency of legal persons and arrangements and to ensure that financial institutions and DNFBPs comply with the AML/CFT Law requirements related to beneficial ownership.

115. In the course of the on-site visit, the assessors arrived at the conclusion that the consolidated CFT efforts taken by the authorities have led to significant improvement of the criminal environment since 2017, and, at present, the **TF risks** could be assessed a medium. The assessors considered the level of coordination and effectiveness of actions taken by the competent authorities to detect and disrupt TF activities, consistency of the undertaken CFT efforts with the risks, vulnerabilities and threats identified in the NRA, and cooperation of the competent authorities with the FIU in the fight against terrorist financing.

116. The main threats emanate from the following types of persons or groups of persons who employ or may employ different methods of raising and using funds for TF purposes:

- Adherents of non-traditional (destructive) religious movements or new trends in Islam – fringe persons or groups that obtain fake or distorted information in the Internet and in different messaging apps;
- The Kazakhs citizens who independently travel abroad (inter alia, to countries with terrorist activities) for religious education;
- The Kazakhs citizens who travel to regions with increased terrorist activities for joining international terrorist organizations, and return from such regions;
- Members of terrorist organizations, illegal armed and radical groups who stay outside Kazakhstan and recruit and engage the Kazakh citizens in terrorist activities via the Internet.

117. No terrorist acts were committed in Kazakhstan in 2017-2021, although, 11 terrorist attacks, some of which caused human deaths, were carried out in 2011-2016. Besides that, large number of foreign terrorist fighters of Kazakh origin (around 450 persons) left Kazakhstan for joining the ISIL in Syria and Iraq (apprx. 450 people) . At the same time, the Republic of Kazakhstan conducted Operation “Zhusan” between 2018 and 2021 and evacuated Kazakh participants of illegal armed groups detained in Syria, as well as Kazakh women and children. A total of 607 fellow citizens were removed to Kazakhstan.

118. TF offences are typically committed with the use of funds from legitimate sources: offenders carry out wire transfers, use bank cards and payment service providers (money transfers without opening bank accounts). Besides that, virtual assets and NPOs could potentially be used for TF purposes, although no such instances were recorded by the competent authorities in practice.

119. The assessment team focused on the effectiveness of measures to combat TF in all its forms, including the financing of FTFs, implementation of TFS, and the integration of CFT in the broader counterterrorism strategy. The assessors also considered the ability of the competent authorities to respond to new complex TF methods, the level of international cooperation for detecting cross-border TF schemes, and the extent to which the efforts of the competent authorities aimed at preventing, identifying, disrupting and prosecuting terrorism-related crimes mitigate the terrorist threat.

120. **Risks of misuse of NPOs for TF purposes** arise primarily from the existing possibility to collect (or) move cash. Non-profit organizations often use poorly controlled methods of raising donations such as: cash deposits into NPOs cash registers or bank accounts, collecting cash into donation boxes, use of bank cards and mobile apps, raising donations through intermediaries who may be temporary employees (such as volunteers and foreign partners) that are rarely subject to a vetting process.

121. Besides that, the assessment team considered the effectiveness of actions taken for preventing misuse of NPO for TF purposes with the application of a risk-based approach. In particular, the assessors verified the powers of the supervisory authorities to audit NPOs and their expenses for identifying risks of their misuse for TF purposes and how such audits are conducted in practice.

122. In addition to that, the application of **TF/PF-related targeted financial sanctions** was identified by the assessors as an issue for enhanced focus. In 2020-2022, Kazakhstan amended the legislation to improve the mechanism of implementation of TF/PF-related targeted financial sanctions so that TFS are applied" without delay". The regulations governing the TFS application procedures were adopted immediately before the on-site visit. The assessors focused on practical implementation of the TFS regime by both large and small financial institutions as well as by the DNFBP and VASP sector entities. Given that there are 4 different lists used in the Kazakh TFS system (international list of terrorists; national list of terrorists and extremists; list of persons linked to terrorism designated by third countries; and list of persons linked to proliferation financing), the assessor deemed it important to consider the ability of private sector entities to effectively identify designated persons, implement freezing measures, provide access to frozen assets in a timely manner (in situations provided for in the FATF Standards), and identify ultimate beneficial owners. Since large number of the Kazakh citizens travelled abroad to fight in the ranks of international terrorist organizations, and also in view of large number of persons included into the national list of terrorists, the assessors considered issues related to international cooperation, *inter alia* with the UN bodies, for inclusion of the Kazakh citizens linked to terrorist activities into the relevant sanction lists. When reviewing the effectiveness of implementation of the PF-related targeted financial sanctions, the assessors also considered the operation of the customs and export control system as the key element of the entire non-proliferation regime.

123. Kazakhstan has also **assessed the PF-related risks**. Although the current round of mutual evaluations[3] does not address PF risks, the assessors noted that a separate PF risk assessment was a positive development. The PF risk factors in Kazakhstan are related to the following:

- Geographical and regional vicinity of the country to the DPRK and Iran;
- Proceeds from criminal activities, organized crime could potentially be used for financing the development and proliferation of weapons, including WMD, in conflict-affected areas.

1.2. Materiality

124. At year-end 2021, the gross domestic product (GDP) of Kazakhstan increased up to USD 191 billion (4.4% growth versus 2020). The real sectors of the economy and certain types of services demonstrated a positive growth rate: construction sector – 11.2 percent; information and communications sector – 8.6 percent; agriculture –5.6 percent; processing industry – 3.9 percent; and educational sector – 2.3 percent.

125. The main exported goods include products of the mining, fuel and energy, metallurgical, chemical and grain industries. The major trade partners of Kazakhstan are Russia, China, the European countries and the CIS member countries.

126. Kazakhstan is not a major financial center or center for company formation and administration, although it is the largest economy in the Central Asia and functions as a regional hub for the Eurasian Economic Union countries, giving it some exposure to cross-border ML and TF risks.

127. One of the contextual factors worth mentioning is the existence of a large "shadow" (informal) economy, which could make it easier for criminals to disguise and conceal their large-scale criminal activities. According to FMA[4], due to the measures taken, the level of "shadow" economy has decreased from 23% to 19% over the past three years. Overall 857 cases have been investigated, and 33 organised criminal groups have been eliminated, and 88 billion KZT in damages have been recovered as part of the combat against the informal economy. 53 billion KZT were compensated out of damages exceeding 57 billion KZT in the area of budget funds embezzlement. Raiding, unjustified increases in utility rates, the illegal export of petroleum and food price speculation were suppressed, and early detection of financial pyramid schemes was improved.

[3] The evaluation was conducted with the use of the FATF 4th Round Methodology and the EAG 2nd Round ME Procedure
[4] The head of state received the chairman of the Financial Monitoring Agency (newsline.kz)

128. Astana International Financial Center (the AIFC) is a unique regional business and financial hub that links the economies of the Central Asia, the Caucasus, the Eurasian Economic Union (EAEU), the Middle East, West China, Mongolia and Europe. The AIFC operates in the country in accordance with the article 2 par 3-2 of the Constitution of the Republic of Kazakhstan. The AIFC aims to evolve into a leading international financial service center. The AIFC objectives are to attract investments in the Kazakh economy, develop the securities, insurance and banking markets, promote Islamic banking, FinTech and E-commerce, implement innovative projects, and integrate the Kazakh economy into the global capital market. The AIFC is limited both by territory and by persons. The AIFC operates under a special legal regime based on the Common Law (of England and Wales) and/or the standards of the major international financial centers. Most AIFC member companies started their operations in 2019-2020.

1.3. Structural Elements

129. Kazakhstan has all of the key structural elements required for an effective AML/CFT system, including political and institutional stability, a high-level commitment to address AML/CFT issues across various parts of government, governmental accountability, rule of law, and a professional judiciary.

130. The implemented reforms are aimed primarily at enhancing the effectiveness of the system and improving the coordination among its stakeholders. The political system and institutional framework are stable. The authorities express a high-level commitment to AML/CFT issues. Significant efforts are undertaken to ensure government accountability, guarantee the rule of law and enhance the independence of a judicial system.

1.4. Background and Other Contextual Factors

131. The provisions of the Constitution, the laws, other regulatory and legislative acts, international agreements and other commitments of Kazakhstan, as well as resolutions of the Constitutional Council and the Supreme Court are the primary sources of law in Kazakhstan. The Constitution is the fundamental law that has the supreme legal force and direct effect.

132. The AML/CFT legal framework, the AML/CFT powers and responsibilities of obliged entities (that are subject to financial monitoring), FMA and other government authorities and the mechanisms of implementation of targeted financial sanctions aimed at preventing and suppressing terrorism, terrorist financing, proliferation and proliferation financing are set out in the AML/CFT Law (as amended by RK Law 88-VII).

1.4.1. AML/CFT strategy

133. The national AML/CFT/CPF system of Kazakhstan is a combination of government, law enforcement and special authorities as well as obliged entities engaged in transactions with funds and (or) other assets (that are subject to financial monitoring) that cooperate with each other within their respective purview.

134. Pursuant to Art.11-1 of the AML/CFT Law, Kazakhstan conducted two national ML/TF risk assessments in 2018 and 2021, respectively. Based on the 2018 NRA findings, the ML/TF risk mitigation measures adopted by RK Government Resolution No.602 dated August 16, 2019 were developed and implemented. At present, the authorities draft a new set of measures to mitigate the ML/TF risks identified in the 2021 NRA.

135. The Financial Monitoring Agency (FMA) coordinated the process of 2021 national risk assessments and preparation for the mutual evaluation. The mutual evaluation process is coordinated by the AML/CFT Interagency Council and the specially established Working Group on Risk Assessment and Mutual Evaluation, which is composed of the representatives of all government, law enforcement and special authorities.

136. Based on the results of NRA, measures aimed at mitigating the risk of money laundering and terrorist financing were developed and approved by the Decree of the Government of the Republic of Kazakhstan

№ 915 on December 20, 2021.

137. Besides that, the following documents are in force in Kazakhstan:

- Concept of Development of Financial Sector of the Republic of Kazakhstan until 2030 adopted by RF Government Resolution No.954 dated August 27, 2014;
- Anti-Corruption Strategy of the Republic of Kazakhstan for 2015-2025 adopted by RK Presidential Decree No.986 dated December 26, 2014;
- Strategy of Cybersecurity of Financial Sector of the Republic of Kazakhstan for 2018 - 2022 adopted by National Bank Board Resolution No.281 dated October 29, 2018;
- State Program of Combating Religious Extremism and Terrorism in the Republic of Kazakhstan for 2018-2022 adopted by RK Government Resolution No.124 dated March 15, 2018;
- Interstate Program of Joint Measures to Combat Crime for 2019-2023 adopted by the Resolution of the Council of Heads of the CIS Member States on the Interstate Program of Joint Measures to Combat Crime for 2019-2023 dated September 28, 2018;
- Strategic Plan of the Agency of the Republic of Kazakhstan for Regulation and Development of Financial Market for 2020-2024 adopted by Agency Chairman's Order No.148 dated February 28, 2020;
- Agreement between the Government, National Bank and Agency for Regulation and Development of Financial Market of the Republic of Kazakhstan on Coordination of Macroeconomic Policy for 2021 – 2023, and Roadmap for Implementation of the Agreement between the Government, National Bank and Agency for Regulation and Development of Financial Market of the Republic of Kazakhstan on Coordination of Macroeconomic Policy for 2021 – 2023 adopted by RK Government Resolution No.90 dated February 23, 2021;
- Action Plan of the Government of the Republic of Kazakhstan for Combating Human Trafficking-Related Crimes for 2021-2023 adopted by RK Government Resolution No.94 dated February 24, 2021;
- National Security Strategy of the Republic of Kazakhstan adopted by RK Presidential Decree dated June 17, 2021;
- 2021-2025 Action Plan for Implementation of the Anti-Corruption Strategy of the Republic of Kazakhstan adopted by RK Government Resolution No.576 dated August 24, 2021;
- Comprehensive Action Plan for Suppressing Shadow Economy for 2021-2023 adopted by RK Government Resolution No.644 dated September 21, 2021; and other documents

1.4.2. Legal and institutional framework

138. The President is the head of the state and the highest official of Kazakhstan who determines the nation's domestic and foreign policies and ensures proper operation of all government authorities. The executive power (including all competent AML/CFT authorities) is exercised by the Government headed by a Prime Minister who is appointed by the President in consultation with the Parliament. The Prime Minister serves as a head of the executive bodies and supervises their activities. The Parliament, consisting of two chambers – the Senate and the Majilis, is the national supreme representative legislative body. The Supreme Court is the highest judicial body of Kazakhstan.

139. The legal system of Kazakhstan is based on the civil law traditions. The primary sources of law in Kazakhstan are:

- Legislative acts: Constitutional Laws; Presidential Decrees having the force of constitutional law; Codes; Ordinary Laws; Presidential Decrees having the force of ordinary law; Resolutions of the Parliament; and Resolutions of the Senate and Majilis;
- Regulations: Regulatory Decrees of the President; Regulatory Resolutions of the Government; Regulatory Orders of Ministers and Heads of other Central Government Authorities; Regulatory Resolutions of Central Government Authorities; and Regulatory Resolutions of the Central Election Commission.

140. The AML/CFT measures are set out in the national legislation, in particular:

- Criminal prosecution measures are set out in the Criminal Code and the Criminal Procedure Code;
- AML/CFT legal framework, powers and responsibilities of obliged entities (that are subject to financial monitoring), the Financial Monitoring Agency and other AML/CFT competent authorities as well as preventive measures and targeted financial sanctions are set out in the AML/CFT Law dated August 28, 2009;
- Some AML/CFT requirements are set out in sectoral laws and regulations issued by specific competent authorities.

141. In Kazakhstan, the AML/CFT institutional framework includes a range of Ministries and Executive Bodies. With a view to coordinating the AML/CFT efforts, the Standing AML/CFT Interagency Council (IAC) was established in November 2020 and became a dialogue platform for development of the national AML/CFT policy. The IAC is composed of the deputy heads of competent authorities and is chaired by the First Deputy Chairman of the Financial Monitoring Agency.

142. With a view to preparing and conducting the mutual evaluation under the second round of the EAG peer assessments, the Interagency Working group was established under the auspices of the Presidential Executive Office.

143. The national AML/CFT system stakeholders include:

144. **Financial Monitoring Agency (FMA)** The FMA is a government authority directly subordinated and accountable to the RK President and is responsible for steering and coordinating the AML/CFT efforts as well as for preventing, detecting, disrupting, solving and investigating economic and financial offences that fall within its jurisdiction under the RK legislation (Presidential Decree No.501 on Measures for Further Improvement of the RK State Governance System dated January 28, 2021). Before signing this Decree the functions of financial intelligence unit were carried out by the Committee on financial monitoring, which was a department of the Ministry of Finance of the Republic of Kazakhstan (Government Decree of 24 April 2008 № 387 "On some issues of the Ministry of Finance of the Republic of Kazakhstan").

Thus FMA is the FIU of the Republic of Kazakhstan. In the Republic of Kazakhstan FMA is a state body with all the powers and functions of FIU (see R. 29), and also performs additional functions on conducting investigations. This function is carried out by the Economic Investigation Service (EIS FMA), which together with its territorial departments forms an operational and investigative unit, carrying out activities for prevention, detection, suppression, detection and investigation of crimes and offenses. The EIS FMA, like the prosecution, internal affairs and anti-corruption services, is a law enforcement agency. EIS FMA interacts with the FMA within its competence on a general basis in accordance with the legislation.

145. **Agency for Regulation and Development of Financial Market (ARDFM)** monitors and supervises most financial institutions (STBs, entities engaged in certain types of banking operations (including KazPost), insurance and reinsurance companies as well as insurance brokers, entities engaged in microfinance activities and professional securities market participants) from 1 January 2020 in accordance with the Presidential Decree 203.

146. **Astana International Financial Center Financial Services Authority (AFSA)** The AFSA is an independent regulator of both financial and non-financial services. It regulates the activities of the AIFC members that provide financial and related services as well as the activities of VAPSs and trusts in the AIFC.

147. **National Bank (NB)** The NB (the first tier bank) is the Central Bank of the Kazakh banking system. Before 2020, the NB supervised and monitored the financial sector, including compliance with AML/CFT requirements. From 2020, the NB is the supervisory authority for payment service providers and non-banking exchange offices.NB

148. **Internal Public Audit Committee of the Ministry of Finance (IPAC)** The IPAC performs

AML/CFT monitoring of audit firms. IPAC's tasks include maintaining state assets, analyzing, assessing and verifying the reliability and validity of financial and management information, the efficiency of internal processes of the organisation of state authorities' activities, etc.

149. **State Revenue Committee of the Ministry of Finance (SRC)** The SRC is responsible, among other things, for customs administration. It verifies and enforces compliance with the customs legislation of the Eurasian Economic Union and the Republic of Kazakhstan and ensures that all customs payments, taxes and other duties are paid in full and in timely manner. Under the non-proliferation regime, the SRC reviews all cross-border transactions related to movement of goods across the customs border and may implement administrative freezing measures for an indefinite period of time.

150. **Agency for Protection and Development of Competition (APDC)** The APDC performs public monitoring and licensing of commodity exchanges starting from September 2020. Previously, the Ministry of national economy supervised commodity exchanges (2018) and the Ministry of trade and integration (2019).

151. **Ministry of Culture and Sports (MCS)** The MCS is responsible for public governance and administration in the fields of culture, state symbols, archiving and documentation, electronic document management and archiving, physical culture and sports, gambling, as well as performs the intersectoral coordination and government regulation functions. The MCS monitors the compliance of the organizers of gambling industry with the AML/CFT legislation.

152. **Ministry of Justice (MoJ)** The MoJ is responsible for AML/CFT monitoring of notaries who provide notary services involving currency and (or) other assets. The Council of Bar Association arranges for compliance by lawyers with the AML/CFT legislations. Lawyers and other independent legal professionals are licensed by the MoJ.

153. **Ministry of Trade and Integration (MTI)** The MTI is responsible for development and promotion of exchange and electronic commerce.

154. **Ministry of Digital Development, Innovation and Aerospace Industry (MDD)** The MDD is responsible for AML/CFT monitoring of activities of VASPs in the country, except those in AIFC territory.

155. **Ministry of Healthcare (MoH)** The MoH is responsible for monitoring the activity of the Social Health Insurance Fund.

156. **General Prosecutor's Office (GPO)** and its local offices supervise precise and consistent compliance with the national legislation, including the AML/CFT legislation.

157. **Ministry of Internal Affairs (MIA)** The MIA is an executive government authority tasked with steering and coordinating the activities of all national internal affairs bodies aimed at combating crime, safeguarding public order and ensuring public security as provided for in the legislation. Structurally, the Ministry of Internal Affairs includes the Police, the Migration Service and the National Guard.

158. **National Security Committee (NSC)** The NSC is responsible for steering and coordinating the activities of all national security bodies. It oversees intelligence, counter-intelligence and criminal intelligence activities, protection of the state border, and operation of the government communication service and "A" commando unit. The NSC coordinates the efforts of all agencies falling within its purview and pursues a single state secret protection policy.

159. **Border Service of the National Security Committee** is responsible for guarding and protecting the land, sea and inland waterway (including underwater) borders of Kazakhstan in order to ensure the integrity and inviolability of the state borders and maintain rule of law and order at the borders.

160. **Anti-Corruption Agency (ACA)** is a government anti-corruption authority directly subordinated and accountable to the President of the Republic of Kazakhstan. The ACA is responsible for developing and pursuing the anti-corruption policy, coordinating the anti-corruption efforts and detecting, suppressing, solving and investigating corruption-related offences.

161. **Supreme court (SC),** local, special and other courts established in accordance with the Constitution and the Constitutional Law on Judicial System and Status of Judges make judgments and decisions under the instituted criminal proceedings, including those related to ML/TF.

162. **Ministry of Information and Social Development (MISD)** The MISD is responsible for public governance and administration in the fields of information, philanthropy, religion, volunteering, mediation, religious and interethnic tolerance, modernization of public consciousness, internal stability, national youth and family policy and interaction between the state and civil society. It also performs the intersectoral coordination and government regulation functions as provided for by the legislation. The MISD analyzes and monitors the activities of non-profit organizations to identify terrorist financing risks and submits such information to the AML/CFT authorized body.

163. **Ministry of Industry and Infrastructure Development (MIID)** Since November 2020, the MIID is responsible for licensing certain types of activities and certain types of goods as well as for coordinating the efforts aimed at marking and tracing (dual-use) goods in the regulated sectors. This function is discharged by the MIID Industrial Development Committee.

164. **Ministry of Economy (ME)** Since November 2020, the ME is the AML/CFT stakeholder and is responsible for government supervision and oversight in the nuclear energy sector as part of the non-proliferation regime. This function is discharged by the ME Nuclear Energy Supervision and Oversight Committee.

165. **Ministry o Foreign Affairs (MFA)** The MFA is responsible maintaining international relations and pursuing the single foreign policy as well as for signing and implementing international treaties and agreements.

1.4.3. Financial sector, DNFBPs and VASPs

166. This section gives general information about the size and makeup of the FI and DNFBP and VASP sectors in Kazakhstan. All sectors presented in this report are described in the FATF Glossary. These are not all of equal importance given their role and size within Kazakhstan, and their different levels of exposure to ML and TF risks. The level of risk also varies greatly between different individual FIs and DNFPBs within the same sector. Assessors ranked the sectors based on the relative importance, materiality and the level of risk. These rankings have been used to weight positive and negative implementation issues throughout the report, as a basis for assessors' conclusions – particularly under IO.3 and IO.4.

Financial sector

167. The financial sector is weighted as the most important sector in Kazakhstan's financial system in terms of volume and value of assets and transactions. The assessors identified the following sectors within the financial sector as important, reflecting both their size and their degree of exposure to ML and TF risks:

168. **Banking sector**: As of July 1, 2022, a total of 22 STB operated in Kazakhstan, including one 100% government owned bank and 13 banks (or 49%) with foreign capital (11 of which are subsidiary banks). The banking sector's assets are 84% of the total assets of the financial sector. The STB operate under the Law on Banks and Banking Activities.

Table A. Number of Second-Tier Banks

#	Indicators/ Years	2017	2018	2019	2020	2021	01.07.2022
1.	Second-tier banks, including:	32	28	27	26	22	22
2.	STBs with foreign capital	13	14	14	15	14	13
3.	Assets, KZT billion	24,220.5	25,241.0	26,800.9	31,171.7	37,622.0	39, 228.6[5]
4.	Loan portfolio, KZT billion	13,590.5	13,762.7	14,743.0	15,792.1	20,200.4	20,649.4[6]

[5] As of July 1, 2022 (https://nationalbank.kz/ru/news/svedeniya-o-sobstvennom-kapitale/rubrics/1706)
[6] As of July 1, 2022 (https://nationalbank.kz/ru/news/svedeniya-o-sobstvennom-kapitale/rubrics/1706)

169. **Securities market**: Brokers/dealers (including STB licensed to perform broker/dealer activities and Kazpost), custodians, investment portfolio managers, transfer agents, the stock exchange (KASE), and the Central Depository can provide services on the financial market. There are investment mutual funds and equity funds, which are not obliged entities but are under the management of investment portfolio managers licensed in Kazakhstan. As of July 1, 2022, the combined assets of investment portfolio managers and brokers/dealers amounted to KZT 510 billion (~$1.2 billion), or 1% of financial sector assets. The number of retail investors in the stock market reached 523 thousand in 2022. The ML risk for securities market participants is assessed as moderate, the TF risk as low. Given the objective characteristics of securities market transactions (high volume of transactions in a short period of time, client confidentiality requirements for brokers/dealers, liquidity, international nature of markets) and the broad client base, securities market participants sector is identified as important.

Table B. Number of Securities Market Participants

#	Indicators/ Years	2017	2018	2019	2020	2021	01.07.2022
1.	Brokers – dealers, including:	45	39	39	37	38	39
2.	Second-tier banks	23	19	19	17	16	16
3.	Non-bank financial institutions	22	20	20	20	22	23
4.	Custodians	10	9	9	9	9	9
5.	Investment portfolio management entities	21	20	20	19	19	20
6.	Transfer agents	2	2	2	2	3	3
7.	Securities trading platform	1	1	1	1	1	1
8.	Financial instruments clearing house	1	1	1	1	1	1
9.	Central securities depository	1	1	1	1	1	1

170. **Entities engaged in microfinance activities (EEMA)**. In accordance with the Law of 26 November 2012 No. 56-V "On microfinance activities" organizations engaged in microfinance activities are microfinance organizations (MFOs), credit partnerships (CPs), pawnshops which carry out activities on granting microcredits. Prior to 2020, registration was mandatory only for MFOs; in 2020, all EEMA, including pawnshops, CPs and online lending companies, were included in the regulatory framework of the ARDFM. From 2021, microfinance licensing is introduced and as a consequence, EEMA are included in the AML/CFT supervisory perimeter of the ARDFM. As of July 1, 2022, 1,044 EEMAs are registered in the Republic of Kazakhstan. As of the middle of 2022, assets amounted to 1.848 billion KZT (~3.9 billion USD or 4% of financial sector assets), of which the largest share was held by MFOs and CPs. The clients of the EEMA are individuals who are residents of the Republic of Kazakhstan. The AML/CFT risk in the activities of EEMA is assessed by the ARDFM as high due to the identified cases of third-party lending, the number of detected violations, as well as the rapid growth of the sector. Given that the RBA in supervising EEMA is at an early stage, EEMA sector is recognized as important.

171. **Postal operators**: In Kazakhstan, there is only one postal operator – KazPost that operates under the KR Law on Postal Service. KazPost provides a wide range of postal and financial services, including postal transfers, banking operations (deposits, opening and maintaining bank accounts, cash operations, opening and maintaining correspondent accounts, foreign currency exchange operations, transfer operations) and broker/dealer services. KazPost carries out banking operations, except for deposits and broker/dealer activities, without an ARDFM license. Starting from May 2020, Kazpost opens and maintains bank accounts of individuals included in the list of entities and individuals involved in terrorist and extremist activities. As of July 1, 2022 KazPost's assets amounted to 143.6 billion KZT (~$346.3 mln). Given the wide range of services, including banking and MVTS, as well as its high risk customer base, the sector of postal services is identified as important.

172. The following sectors were weighted as moderately important:

173. **Insurance sector**: As of July 1, 2022, there were 27 insurance companies and 9 insurance brokers operating in Kazakhstan under the RK Law on Insurance Activities. As of July 1, 2022, the assets of insurance (reinsurance) companies amounted to 1.980 billion KZT (~$4.2 billion) or 4% of financial sector assets. The total number of deals reached 10 million, of which 86% were with individuals. The bulk of

contracts and premiums relate to property risk insurance and compulsory insurance. In 2022 life insurance premiums amounted to 237 billion KZT (~$504 mln), and this sector is rapidly growing. Given the small volume of the life insurance sector, the moderate/low ML/TF risk identified in the SRA, and the national insurance market context of Kazakhstan (low risk of nonresident tax money laundering), the insurance sector is identified as moderately important.

Table C. Number of Insurance Sector Entities

#	Indicators/ Years	2017	2018	2019	2020	2021	01.07.2022
1.	Insurance companies, including:	32	29	28	28	27	27
2.	Life insurance companies	7	6	8	9	9	9
3.	Insurance brokers	16	15	13	12	10	9
4.	Actuaries	59	56	57	58	60	57
5.	Insurance (reinsurance) companies that are members of the Insurance Payments Guarantee Fund	22	23	25	27	26	26
6.	Representative offices on non-resident insurance companies	3	3	3	3	3	3

174. **Payment service providers (PSP):** Under the Law on Payments and Payment Systems, the payment service providers offer the following types of services: acceptance of cash for making payments without opening bank account; sale (distribution) of e-money and payment (pre-paid) cards; acceptance and processing of e-money payments initiated electronically and transmitting necessary information to banks /institutions engaged in certain types of banking transactions for effecting or receiving payments and (or) money transfers. As of January 1, 2022, there were 93 payment services providers registered in Kazakhstan (91 payment service providers were registered as of July 1, 2022). The volume of payment services provided by PSP was 0.8% of the payment turnover of STB as of 1 July 2022, which represents an insignificant share. There are 19 money transfer systems operating in Kazakhstan, including two national payment systems, payment card systems, as well as seven international money transfer systems that are not obliged entities. Taking into account the relatively small but growing volume of transactions of PSP, the nature of the services provided and their rather high ML/TF vulnerability, as well as the fact that international payment systems are not obliged entities and therefore not subject to the NB's AML/CFT supervision, this sector is identified as a moderately important.

175. **Leasing companies**: Pursuant to RL Law No.78 on Financial Leasing dated July 5, 2000, the Agency for Regulation and Development of Financial Market issues licenses to banks that carry out leasing activities in the capacity of lessors. Other legal entities and individual entrepreneurs are allowed to carry out leasing activities as lessors without a license only after notifying the FMA about launch of this type of activity. Starting from 2020, leasing companies performs as obliged entities and are subject to AML/CFT compliance monitoring by the FMA. As of June 1, 2022, there were 66 entities that carried out leasing activities without licenses. There are no individual entrepreneurs registered in the sector. At the beginning of 2022, the overall amount of leasing deals was almost KZT 477.8 billion (~$1.1 billion). Given the moderate volume of deals and moderate risk of client base (mainly resident entrepreneurs and legal entities) and taking into account the lack of license and absence of AML/CFT compliance supervisor until 2020, the leasing companies sector is identified as moderately important.

176. **Exchange offices**: As of June 1, 2022, there were 2,109 exchange offices in Kazakhstan, including 1,440 bank exchange offices, 433 exchange offices run by the authorized institutions (AI) and 236 KazPost exchange offices, that operated under the Law on Foreign Exchange Regulation and Control. The total amount of foreign exchange transactions by AIs with individuals in 2022 was 5.467 billion KZT (~$11.6 billion). Compliance with AML/CFT requirements by banking and Kazpost's exchange offices is carried out by the ARDFM, while the NB supervises other AIs. Given the rather large number and relatively high percentage of high-risk AIs, taking into account the average ML/TF risk identified by the NB and the limited nature of operations, the AIs sector is recognized as moderately important.

177. Other sectors were weighted as being of low importance. These include:

178. **Entities engaged in certain types of banking operations (EECTBO):** Non-banking organisations may carry out certain types of banking operations provided for in the Law on Banks and Banking Activities, provided they have the appropriate license. As of July 1, 2022, the non-banking financial sector of Kazakhstan included 2 mortgage companies and 3 entities engaged in certain types of banking operations . The assets of EECTBOs amount to 2.902 billion KZT (~$6.2 billion) or 6% of the financial sector's assets. Their main activity concerns the provision of loans to retail and corporate customers. Taking into account the limited activities of the EECTBO, as well as the low level of AML/CFT risk identified in the SRA, the sector is identified as low important.

179. **Commodity exchanges**: In accordance with AML/CFT legislation commodity exchanges are obliged entities. Commodity exchanges in Kazakhstan carry out their activities on the basis of the Law On Commodity Exchanges, and starting from the middle of 2020 they are supervised by the APDC in terms of AML/CFT compliance. According to the Ministry of Trade and Integration, as of July 1, 2022, there were 17 commodity exchanges. In 2019-2020, four commodity exchanges were inactive and carried out no exchange transactions, while in 2018, the commodity exchanges carried out a total of 5 transactions with overall amount of KZT 850 million (~$2,4 million). Given the specification of commodity exchanges and the low ML/TF risk identified in the NRA report, the sector is given a low importance.

180. **AIFC members operating in/from AIFC:** As of July 2022, the AFSA issued licenses to 62 authorized companies and 3 authorized market institutions, including the stock exchange with 20 member companies, the Central Depository and crowdfunding platform. The authorized companies are primarily engaged in investment activities, including collective investment portfolio management; 6 companies carry out banking activities, 4 companies provide insurance services; and remaining companies are engaged in other types of regulated activities.

181. At the moment of the mutual assessment, the financial sector assets of AIFC amounted to USD 1.2 billion or 1,31% of total assets of the financial sector in Kazakhstan. The assets of banking sector of AIFC (USD 1.1 billion) accounted for 1,46% of assets of the country's banking sector. The STB in AIFC do not provide services to the individuals.

182. The volume of the attracted equity capital at the stock exchange amounted to USD 321 million, and the trading volume totaled USD 298.5 million. Total value of managed assets reached USD 736 million.

DNFBP sector

183. The assessors identified the following DNFBP sectors as important based on the results of NRA-2018 and NRA-2021:

184. **Individual and corporate dealers in precious metals, precious stones and jewelry (jewelers):** As of July 2022, 496 jewelers are active in Kazakhstan. 247 entities are newly registered. In order to start an activity as obliged entities, 496 of them submitted the mandatory notification to FMA. Production and sale of precious metals, precious stones and raw materials, jewelry and other items containing precious metals and precious stones is regulated by the RK Law on Precious Metals and Precious Stones. The market for precious metals and stones is regulated by the state, and the price of precious metals and stones is set by the state (see para 111). Dealers in precious metals and stones are the obliged entities.

185. **Individual and corporate real estate agents**: There are 424 real estate companies and real estate agents in Kazakhstan actively conducting real estate activities, which submitted the mandatory notification to FMA. Real estate agents are participants of the real estate sector but are not involved in the financial aspects of transactions. They provide real estate selection services and assistance in preparing documents (see para 111). Real estate agents are the obliged entities.

186. **Organisers of gambling industry**: According to the legislation the organisers of gambling industry are casinos, gaming machine halls, bookmaker offices, totalizators. All are obliged entities and must comply with the requirements of the AML/CFT Law. The privilege to organise and conduct gambling is granted exclusively to legal entities of Kazakhstan, which are entitled to conduct activities in gambling industry

based on the license. Electronic casinos and online casinos are officially illegal in Kazakhstan. There are no ship-based casinos in Kazakhstan (see para 111). As of 1 January 2022, there were 6 casinos and 51 other organizers of gambling industry. As of 1 July 2022 the number of other organisers reduced to 48. In addition, there is 1 lottery operator in the Republic of Kazakhstan, which has been assessed along with casinos and other organisers of gambling industry in the NRA 2021.

187. The following sectors were identified as moderately important due to the number of subjects and results of NRA-2018 and NRA-2021:

188. **Notaries**: As of on-site mission there were 4584 notaries registered in Kazakhstan. The number of registered notaries increased up to 4,381 by January 1, 2022 and reached 4,482 by July 1, 2022. Notary activities are licensed by the Ministry of Justice that keeps the State Register of issued notary licenses and publishes information on licensed notaries in its official journal. In Kazakhstan, notaries operate under the Law No.155 on Notaries. Notaries public certify deals in real estate sector but are not involved in the financial aspects of transactions. Notaries who provide notary services involving currency and (or) other assets are the obliged entities.

189. **Accounting firms and individual professional accountants**: There are 1,038 accounting firms registered in Kazakhstan, which operation is regulated by the RK Law on Accounting and Financial Reporting. In addition to the results of the NRA 2021, whish rated the sector as medium risk, the criteria for assessing the sector's weighting include: significant growth in AML/CFT involvement in the sector (from 84 organisations in 2018 to 1,038 organisations in 2021). As stated in the NRA 2021, the knowledge and expertise of the sector can be used for complex financial transactions, minimising the tax burden. However, no evidence was presented that members of this sector have been used for ML/TF purposes. All of them are the obliged entities.

190. The following sectors were weighted as being of low importance due to limited range of financial transactions:

191. **Lawyers, legal advisors and other independent legal professionals**. Activities of the lawyers, legal advisors and other independent legal professionals are regulated by the Law on Legal Practice and Legal Assistance. A person needs to obtain a license for practicing law. Lawyers and legal advisors provide a very narrow range of services in the context of FATF Recommendations. As of July 1, 2022, there were 5,732 lawyers, and 866 legal advisors and other independent legal professionals actively performed their activities in Kazakhstan. They all are obliged entities.

192. **Audit firms** are obliged entities in accordance with the AML/CFT Law. The activities of audit firms shall be licensed. An auditor must pass a qualification examination and may only carry out his/her activities in an audit firm. In Kazakhstan, as of 1 January 2022, 1,869 licenses to engage in auditing were issued, and 478 audit firms were registered. 7 professional associations unite all audit firms. The audit firms operate as per the Law on Audit Activity.

193. AIFC members: DNFBP – providers of trust services and ancillary services whose business or profession is conducted to/from AIFC, trusts. Only providers of ancillary services (legal, audit, accounting, advisory and credit rating) are registered in AIFC, 148 or 10% of the total number of companies registered with AIFC from 2019 to August 2022, of which 114 are active. Trusts and providers of trust services can be registered with AIFC, as of on-site mission there were none. All the listed categories of the AIFC members are obliged entities.

194. There are no independent professions providing trust services and company services (TCSP) in Kazakhstan, except for AIFC members, as well as legal advisors, independent legal advisors, independent legal professionals, who may serve as agents in the establishment of legal persons. In addition, certain securities market prticipants (the central depository, custodian and broker and/or dealer authorised to maintain customer accounts as a nominee for securities, organisation registering securities transactions with the AIFC, and single operator for the nomination of securities held by government, quasi-public sector entities) may act as a nominee for securities.

VASPs and virtual asset transactions

195. The sector's activity is categorized as of moderate priority. Transactions with virtual assets are to a limited extent permitted business activities in Kazakhstan. There are two types of VASPs that fall into the category of obliged entities that are subject to financial monitoring:

- VASPs that carry out certain types of business activities determined by the AFSA in consultation with the designated government agency in line with the FATF Recommendations. These VASPs are the AIFC members and are covered by the special legal regime in force in the AIFC territory. Activities of AIFC residents are subject to licensing. As of January 1, 2022, there were six registered VASPs, and their number increased up to eight by July 1, 2022. However, only two VASPs are active (i.e. carry out transactions for customers). Based on the assessment, 6 VASPs have a medium risk level (1 crypto-broker and 5 crypto-exchanges) and 2 have got a high risk level (1 crypto-exchange and 1 tokenized securities exchange). The total volume of VASPs transactions in AIFC since August 2022 was around $6 million;
- VASPs that issue digital assets, arrange for trading in digital assets and exchange between digital assets and fiat currency or other assets. For entering the market, an entity involved in these types of activities needs simply to notify the Ministry of Digital Development, Innovation and Aerospace Industry (MDD). However, at the time of the on-site visit, no VASPs of this type operated in Kazakhstan.

1.4.4. Preventive measures

196. According to the AML/CFT Law, all categories of FIs and DNFBPs are the obliged entities covered by the law and are required to take measures for preventing breaches and mitigating ML/TF risks and to report the relevant transactions to the FIU in the course of their activities.

197. A simplified CDD regime, which excludes the obligation of the FIs to identify the BO, applies to state bodies and quasi-public entities.

1.4.5. Legal persons and arrangements

198. Kazakh citizens and foreign nationals may carry out business activities in Kazakhstan through legal persons of different types, such as: general partnerships, limited liability partnerships, partnerships with additional liability, limited (commandite) partnerships, joint-stock companies (corporations), branches and representative offices of business entities. Branches and representative offices of foreign companies are quite intensively-used types of business entities in Kazakhstan.

199. All legal entities created in the territory of Kazakhstan are subject to registration, irrespective of the purpose of their establishment, nature and type of activities and membership. Branches and representative offices of legal entities located in the territory of Kazakhstan are subject to record registration without granting them the status of legal persons. The Ministry of Justice of the Republic of Kazakhstan and its territorial subdivisions are responsible for the registration.

Table D. Number of Legal Persons Registered in Kazakhstan

Legal Persons	2019	2020	2021	I half of 2022
Legal entities	433 774	446 687	461 983	480 799
Individual entrepreneurs	1 204 705	1 198 742	1 180 871	1 367 918
Non-resident legal entities	632	393	237	842
Non-profit organizations	22 141	22 373	22 512	22 742

200. In Kazakhstan, a non-profit organization is defined as a legal entity which primary objective is not generating profits and which does not distribute net income among its members. NPOs may be created in various legal forms, such as: institutions, public associations, joint-stock companies, consumer cooperatives, foundations, religious associations, associations (unions) of legal entities, or in other forms provided for in the legislation.

201. Besides, there is a special registration regime established in the AIFC, where different types of legal persons may be created and registered; These include: private companies, public companies, accredited companies, general partnerships, limited partnerships, limited liability partnerships, accredited general partnerships, accredited limited liability partnerships, special purpose companies, investment companies, non-profit organizations, and private foundations.

Table E. Number of AIFC Member Companies

Type	2018	2019	2020	2021	I half of 2022
Private companies	58	182	240	476	238
Accredited companies	13	19	18	10	7
Limited liability partnerships	3	16	15	23	5
Special purpose companies	0	9	6	16	7
Non-profit corporate organizations	5	18	4	8	9
Public companies	0	0	1	3	0
Investment companies	0	0	1	4	4
Accredited limited liability partnerships	0	3	0	7	1
Private foundations	0	2	0	1	0
Limited partnerships	0	1	0	2	1
Accredited general partnerships	0	1	0	0	0
General partnerships	0	0	0	0	0
Accredited limited partnerships	0	0	0	0	0

202. Express trusts and other similar legal arrangements cannot be created under the Kazakh law. However, nothing prevents a person in Kazakhstan from setting up or managing a legal arrangement created under foreign law. Besides that, trusts and similar legal arrangements can be created in Astana International Financial Center and be the AIFC members. As of on-site mission there were none.

203. As noted in the ML NRA, risks of use of shell/ front legal entities for carrying out illegal financial transactions are quite common, as witnessed by financial investigation findings and completed criminal proceedings related to fictitious (fake) invoices and tax evasion (36% of all ML cases).

1.4.6. Supervisory arrangements

204. Kazakhstan has AML/CFT supervisors for the various sectors and activities covered by the AML/CFT measures. The main supervisory authorities are:

Table F. Supervisory Authorities

Types of Entities	Supervisor
Second-tier banks	ARDFM[7]
Insurance companies, insurance brokers	
Professional securities market participants	
Entities engaged in certain types of banking operations	
KazPost	ARDFM/MDD
Legal advisors and other independent legal professionals	FMA
Leasing companies	
Individual and corporate real estate agents	
Individual and corporate dealers in precious metals, precious stones and jewelry	
Accounting firms and individual professional accountants	
Payment service providers	NB
Licensed corporate operators of exchange offices	
AIFC member companies	AFSA
Organisers of gambling industry	MCS
Audit firms	IPAC
Commodity exchanges	APDC
Notaries	MoJ

[7] Prudential regulation (www.gov.kz)

Lawyers	The Council of Bar Association

1.4.7. International cooperation

205. The General Prosecutor's Office coordinates all MLA-related matters. Cooperation with the CIS member countries is based on two multilateral Conventions – Minsk Convention of 22.01.1993 and Chisinau Convention of 07.10.2002, while cooperation with other countries is based on bilateral agreements. Kazakhstan may also provide mutual legal assistance based on the principle of reciprocity. Besides that, Kazakhstan ratified all basic UN conventions against crime that envisage provision of mutual legal assistance in criminal matters.

206. Kazakhstan directly cooperates with foreign law enforcement agencies, FIUs and supervisory authorities. Information is exchanged most actively and intensively with Russia, USA, France, Kyrgyzstan, Uzbekistan, Latvia, Estonia, Italy, Ukraine and UAE.

CHAPTER 2. NATIONAL AML/CFT POLICY AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

1. The Republic of Kazakhstan used its own methodology to assess ML and FT/PF risks. All competent authorities and the private sector were involved in the preparation of the NRA. To prepare the NRA, a large volume of quantitative and qualitative data was used.

2. The approach used in ML NRA, which enables to assess predicate offences that generate main proceeds and review ML-related criminal cases, highlights the national priorities, but does not contain a conclusion on specific ML risks.

3. The FT/PF NRA clearly highlights the FT risks of the country. The evaluators agree with the findings of the FT/PF NRA on the average risk level, taking into account a number of factors and measures that national competent authorities apply to mitigate the identified risks.

4. In the course of the NRA, the risk assessments of the use of virtual assets and the NPO sector was also conducted; in addition, assessment of the vulnerabilities of legal entities was conducted. However, the NRA does not assess the national cross-border ML risks. Despite this fact, competent authorities and the private sector have demonstrated that they understand the cross-border risks related to cash flow.

5. Following the ML/TF/PF NRA, a number of supervisory authorities also conducted sectoral risk assessments.

6. The national AML/CFT policy is appropriately aimed at taking measures to mitigate the identified ML/TF risks. Kazakhstan implements an ongoing and coordinated process to develop policy based on the outcomes of official risk assessments. Appropriate national strategies and action plans developed, inter alia, based on the 2018 and 2021 ML/TF national risk assessments, are an integral part of the strategic and operational national policy to combat ML/TF in the country.

7. The laws of the Republic of Kazakhstan do not contain provisions that enable not to apply the FATF Recommendations. The outcomes of the NRA are used to identify an ability to apply simplified and enhanced measures by obliged entities.

8. National interaction and cooperation are the strengths of the Kazakh AML/CFT framework. FMA is responsible for coordination of legislative and operational AML/CFT activities and receives a high-level support from the country's leadership. Kazakhstan has various interagency coordination mechanisms.

9. The NRA outcomes are adequately communicated to the private sector through both institutional and operational mechanisms. FIs, DNFBPs and other sectors that should follow the AML/CFT requirements were directly involved in national and sectoral risk assessments.

Recommended actions

1. Continue to improve the methodology of the NRA ML, namely the make an analysis of all predicate crimes that generate criminal income, as well as financial flows that can be linked to organized crime and the transnational dimension.

2. Continue to develop the analysis of ML/TF methods, trends and typologies.

3. Conduct a comprehensive sectoral analysis to better understand the varying degrees of exposure of sectors and organizations to different types of ML/TF risks.

4. Continue to update comprehensive plans and national strategies to reflect updates to the NRA ML and NRA TF/PF.

5. Take into account ML and TF risks identified as a result of NRA when developing a national risk minimization plan. Consider the possibility of preparing a consolidated comprehensive plan to minimize ML/TF risks for a clearer understanding of the identified risks. This measure will also allow for residual risks to be taken into account when updating the NRA.

207. This Chapter considers and assesses the achievement of Immediate Outcome 1. To assess efficiency, this section used Recommendations 1, 2, 33 and 34, as well as the elements of Recommendations 15 are used.

2.2. Immediate outcome 1 (Risk, policy and coordination)

2.2.1. Understanding of the existing ML/TF risks

208. The competent authorities and the obliged entities of the Kazakhstan understand their ML/TF risks to a large extent. The country has made sufficient efforts to identify, understand and assess ML/TF risks, as well as to develop measures to minimize them. The assessors reached this conclusion by reviewing national risk assessment reports, policy and guidance documents, as well as interviews during the on-site mission.

209. The first NRA was conducted in 2018; The NRA 2018 process was coordinated by the Financial Monitoring Commission (subsequently transformed into FMA) within the IMC. In order to conduct the NRA 2018, working groups were formed from representatives of government, law enforcement, supervisory authorities and representatives of the private sector.

210. The 2018 ML/TF NRA identified high-risk areas and predicate crimes that generate criminal proceeds. These crimes included: fraud, tax crimes, corruption and bribery, participation in organized crime and racketeering, extortion, robbery and theft, smuggling and forgery.

211. In addition, the 2018 NRA ML/TF identified vulnerable obliged entities, which included banks and organizations engaged in certain types of banking operations, exchange offices, postal operators, DPMS, certain DNFBPs (accountants and auditors, organizers of gambling industry, individual entrepreneurs).

212. Based on the results of the 2018 NRA, a Plan to minimize these risks was formed, which were approved by Government Decree No. 602 of August 16, 2019. The measures contain a list of preventive, regulatory, law enforcement, organizational measures and measures aimed at improving the effectiveness of interagency cooperation and interaction with the private sector. As a result of the implementation of the above action plan, amendments were made to the AML/CFT legislation, supervisory authorities were identified for certain types of FIs and DNFBPs, and other measures were taken to minimize the risks identified in the course of the NRA.

213. In 2021, two separate NRA were conducted – in respect of ML and in respect of FT/PF; all competent authorities and the private sector were involved in them. For this purpose, own methodology has been developed based on the OSCE Guidance on the collection of data to conduct the ML/TF risk assessment and Words Bank's Risk Assessment Tool. The summary of the both NRA was published on FMA's official web-site and on government authorities' web-sites. The Competent Authorities and the obliged entities agree with the findings of both NRAs and share a view of the largest national risks, threats, and vulnerabilities.

214. As a result of meetings with government officials, the assessors concluded that the competent authorities demonstrated a thorough understanding of the constituent elements of risk and showed that they were aware of the most relevant schemes, methods and tools used for money laundering and terrorist financing.

215. In the course of the ML NRA, large volumes of qualitative and quantitative data from numerous public and private sources were used. To assess risks, various information was used, including different level documents related to risk assessment (strategies and decrees), official crime statistics, outcomes of

monitoring and supervision activities, requests of law enforcement authorities and foreign FIU, financial flows data, typologies, investigative reports, criminal case files, court sentences, results of surveys and mass media materials.

216. The methodology to collect data, under which NRA was conducted, was approved in 2017. Accordingly, the evaluators assume that the Methodology may be improved or revised; also, Kazakhstan could consider new (modern) approach to assess the national risks.

217. The ML NRA identifies threats with a breakdown into the predicate offices committed in the country. Following the review, the most pressing national threats have been identified: bogus invoices, evasion of taxes and customs duties, smuggling, illegal entrepreneurship, illegal gambling, illegal trafficking of oil and oil products, corruption and embezzlement, Ponzi schemes and drug trafficking.

218. To assess the ML risks, apart from the threats, the vulnerabilities of the national AML framework have been identified. They include cash circulation, use of shell companies for ML schemes; cross-border transfers of illegal funds; shortcomings of government authorities and the financial sector' risk management systems; insufficient outreach activities for obliged entities.

219. When threats and vulnerabilities were compared, the major ML risks were identified: misuse of credit institutions (second tire banks) and institutions that make some types of bank transactions; use of shell companies for ML schemes; use of organisers of gambling industry for ML schemes; misuse of microfinance organizations for ML schemes. However, the identified risks are not exhaustive. In addition, the ML NRA lacks the review of the risks of cross-border movement of funds.

220. The TF risks are well identified and clear. The national CFT/CPF framework facilities strengthening of the national security and stability of the financial sector. The TF/PF NRA Report highlights the specific threats that come from the members of non-traditional (destructive) religious movements that receive misleading information from the Internet; nationals of Kazakhstan that leave the country on their own to receive theological education, including to the countries where terrorist activities occur; nationals of Kazakhstan that go to the areas of high terrorist activity to join ITOs and those who return from these areas; members of terrorist organizations and illegal military and radical groups located outside the Kazakhstan that involve Kazakhstani in terrorist activities through the Internet. The risks have been reviewed with respect to vulnerabilities at the three stages of financing of terrorism (collection, movement and use of funds). The TF NRA specifies that in the course of financing of terrorism funds are used that were obtained from legitimate sources: wire transfers, bank cards, payment institution services (money order transfers) as well as digital assets. In addition, the TF NRA contains information on the specific financial profiles of the persons involved in the activities related to financing of terrorism. Misuse of virtual assets and NPOs for TF purposes also raises concerns.

221. The TF/PF NRA is a high-level document; it contains limited information on specific threats. However, understanding of TF/CPF is effectively supplemented by specific knowledge of law enforcement authorities' officials that fight against terrorism. Law enforcement and special government authorities have demonstrated the knowledge of the financial activities of specific organizations and persons that operate in Kazakhstan and aboard and FMA' capabilities to initiate and assist in tracing of funds related to TF and assist in conducting parallel financial investigations as part of TF cases. Good identification results are confirmed by the case studies submitted during the on-site mission. Following investigation of these cases, persons have been convicted for terrorism-related activities.

222. The Kazakhstan makes continuous efforts to update and assess the sectoral risks. In 2022 FMA has conducted additional assessments of the TF risk of the NPO sector, assessment of the legal entities and arrangements' risks with respect of involvement in ML schemes and assessment of the virtual assets sector.

223. Following the assessment of the TF risks in the NPO sector, there have been identified the vulnerabilities related to potential misuse of NPOs for TF, terrorist organizations' misuse of social media to raise funds under the pretext of rendering assistance to people in need, and Syrian refugees, Muslim students who study in Europe, construction of mosques, etc. Upon the findings of the Report, the risk of

the misuse of NPOs in TF schemes is assessed as “medium”; in this connection, a number of measures are envisaged to manage the TF risks of the NPO activities and a number of measures are recommended to mitigate the identified risks.

224. In the course of assessment of the vulnerabilities of legal entities and arrangements to be involved in ML schemes, it was identified that entrepreneurial activities in Kazakhstan is mostly conducted in the form limited liability partnerships (legal entities), private companies (members of AFSA) or as individual entrepreneurs (natural persons). According to law enforcement authorities, one of the issues is the companies’ use of shell companies to evade taxes, MFO’s involvement in fraudulent schemes (Ponzi schemes) and ML and activities in the country without being physically present (branches or representative offices) through web-sites. Deficiencies related to promptness of obtaining and relevance of the data on beneficiary owners increases the vulnerability of Kazakh legal entities up to high level. This report also highlights a number of measures to mitigate the identified risks.

225. In 2021, the AFSA conducted assessments of ML/TF risks in the controlled sectors: DNFBPs and fintech companies, including VASPs. According to the results of the assessment the AIFC participants - DNFBP and VASP were assigned a medium risk level. The risk of using digital assets (cryptocurrency) on the territory of AIFC is also medium.

226. The assessment team concluded that the assessment of the VA sector has identified that its current regulation prescribed by the national laws is sufficient and complies with the FATF requirements. Taking into account a fast growth and popularity of the VA market, the nationals of Kazakhstan actively use Internet-platforms that purchase and sale cryptocurrency, which may be used for illegal purposes. Nationals of Kazakhstan may access VA through foreign and national crypto exchanges, cash exchange services and transfers through online banking services and VASPs registered with AIFC. The appropriate government authorities and entities implement Road Map on Development of Crypto Industry and Blockchain Technologies in Kazakhstan that envisages a pilot project on STB’s servicing of crypto exchanges registered with AFSA and reviews the need to improve laws with respect to regulation of crypto exchanges upon the outcomes of this project. Also, under R.15, Committee of AFSA has developed and implemented Signs/Criteria of Suspicious Virtual Asset Transactions and VASPs. The Government of the Kazakhstan and FMA interact with Binance, the largest crypto exchange in the country. For instance, Memorandum between the Government of the Kazakhstan and Binance prescribes that this crypto exchange will assist in consulting on the development of the legal framework and policies of regulation of VA in Kazakhstan. Following the on-site mission, the evaluators concluded that that Kazakhstan understands the current ML/TF risks related to VA and VASPs.

227. Also, ARDFM conducted a sectoral assessment of the ML risks. NB conducts assessment of the risk levels of PSP and AIs once per six months. Following the assessment of the risk levels, the risk levels of reporting entities are identified, and NB makes a list of high-risk entities (including, high-risk entities in terms of ML/TF/PF).

2.2.2. National policy aimed at mitigating the identified ML/TF risks

228. The national AML/TF policy of the Kazakhstan focuses on the mitigation of the identified ML/TF risks. All relevant national action plans developed based on the results of the national ML/TF risk assessments conducted in 2018 and 2021 are components of the national policy at the strategic and operational level aimed at combating ML/TF. This conclusion was confirmed during the meeting with the members of the Interagency Working Group on the preparation of the Kazakhstan for the second round of the EAG mutual evaluation under the Presidential Administration of the Kazakhstan, where information on the improvement of measures taken since the previous risk assessment, including national AML/CFT legislation with regard to the FATF Recommendations was presented.

229. This conclusion is also supported by a review of action plans and other policy documents. The assessors conclude that all of them significantly minimize the existing ML/TF risks.

230. For instance, National Development Plan for the period up to 2025[8] defines as one of national priority measures that FMA should focus on the fight against shadow economy, which is one of ML/TF preconditions. Currently, Comprehensive Action Plan to Combat Shadow Economy for 2021-2023 approved by the Decree of the Government of the Kazakhstan No. 644 dated September 21, 2021 is implemented. National Security Strategy for 2021-2025[9] and Action Plan to Manage National Security Risks specify as one of the measures introduction of effective financial monitoring system to protect the national economy from ML/TF threats, strengthen the integrity of the financial sector and ensure its protection and safety. One of the tasks of Legal Policy Strategy up to 2030[10], is to separate financial investigations from criminal proceedings.

231. A number of AML/CFT initiatives to ensure national security is implemented under sectoral policy documents. For instance, this year saw the approval of Anticorruption Policy Strategy for 2022 – 2026. The new strategy is a document that focuses on comprehensive and profound work to eliminate the preconditions of corruption; it envisages measures that, as expected, will significantly contribute to the national law enforcement authorities' efforts to combat ML. Fight against fraud is implemented as part of Joint Measures to Combat Fraud and Ponzi Schemes (Road Map) approved by the General Prosecutor of the Kazakhstan. Following the 2018 NRA, MIF of the Kazakhstan annually developed and approved Plan to Prevent, Investigate and Detect Frauds Committed through IT. In addition, the minutes of meeting of Ministry of Information and Social Development (MISD) to develop proposals to combat drug offences and prevent drug addiction chaired by the Deputy Prime Minister of the Kazakhstan approved Road Map to Enhance Fight against Drug Offences and Prevention of Drug Abuse for 2022-2023. Additionally, the Kazakhstan has approved awareness raising activities to prevent drug addiction among people, including youth, for 2022. Also, the GPO of the Kazakhstan in cooperation with MIA, NSC и MISD of the Kazakhstan has approved Interagency Action Plan for 2021-2022 to improve the legal framework and mechanisms of government authorities' interaction to develop and take measures to eliminate the reasons/conditions that contribute to the propaganda and illegal advertising of narcotic drugs.

232. As was noticed above, currently Kazakhstan implements an action plan to combat shadow economy for 2021-2023. The primary objectives of this plan, inter alia, are to prevent smuggling and evasion customs duties and taxes, eliminate false declaration/non-declaration of goods and vehicles moved through the customs border, prevent smuggling of strategic goods and resources, conduct effective and transparent tax administration, ensure fast information sharing between government authorities and STBs, give effective response to combat shell companies, eliminate risks of embezzlement, ensure transparency of the spending of budget funds, comply with regulatory requirements by organisers of gambling industry and comply with regulatory requirements related to entrepreneurial activities.

233. Among the measures taken by competent authorities based on the outcomes of the previous risk assessment, regulatory measures may be highlighted. In particular, to ensure compliance of the national laws with the FATF Standards, in 2020 the Law On Making Amendments in Certain Regulations Related to Combating Legalization (Laundering) of Illegal Proceeds and Financing of Terrorism (№ 325-VI dated May 13, 2020) was adopted that became effective on November 15, 2020. Pursuant to it, FMA has become to regulate five types of obliged entities (real estate agents, lawyers, leasing, accounting companies, professional accountants and jewelers); obliged entities' liability for non-compliance with the requirements of the AML/CFT Law has been increased; mechanisms and procedure for application of TFS for PF by obliged entities and some government authorities have been established; mechanism to coordinate measures to assess risks by the Interagency AML/CFT Board has been established; risk-based approach to examine FMA has been implemented; government authority responsible for registration and use of confiscated assets has been specified and the fund of these assets has been formed; international cooperation related to AML/CFT information sharing between financial control/law enforcement authorities and foreign competent authorities has been enhanced.

[8] The Decree of the President of the Republic of Kazakhstan No. 636 dated February 15, 2018 (Building diversified and innovative economy)
[9] The Decree of the President of the Republic of Kazakhstan dated June 17, 2021.
[10] The Decree of the President of the Republic of Kazakhstan dated October 15, 2021

234. To further improve the AML/CFT framework and following the 2018 and 2021 NRAs, the members of AML system have taken and take comprehensive measures to combat and mitigate the identified ML/TF risks. For instance, ACA has adopted two packages of legislative initiatives. Civil servants, the members of the Parliament of the RK and judges have been prohibited from having foreign accounts; liability for corruption of law enforcement authorities' officials, judges, bribers and bribe intermediaries has been increased; parole for grave and especially grave corruption offences has been cancelled; prohibition has been introduced to direct convicts directly to institutions of minimum safety. Also, candidates for public offices have been obliged to notify of the relatives that work in the same authority; civil servants and other persons that have accepted anticorruption restrictions, as well as members of their families, have been prohibited from receiving gifts, financial rewards and services. Liability for corruption in the quasigovernment sector has been increased. Principles of anti-corruption compliance have been established in national companies and the private sector. Criminal liability of the officials of law enforcement and special government authorities for entrapments has become an important legislative innovation. Amendments have been made in the Criminal Code, which increase the liability of law enforcement officials and judges for obstruction of and unlawful interference into entrepreneurial activities.

235. The Law On Making Amendments in Certain Gambling Regulations has introduced the following amendments: introduction of bet recording center that ensures connection communication networks of software and hardware systems to the software and hardware system of bookmaker offices or totalizators and ensures acceptance (making) payments in cash and noncash form, including through electronic money, acceptance, recording and keeping of information on the accepted bets, including electronic bets, for each member of betting, coefficients of the variants of the results of betting, prizes and payments on them. Specific bets for organisers of gambling industry have been prescribed.

236. To minimize ML/TF risks, the Law On Making Amendments in Certain Regulations related to Mortgage Loans in Foreign Currency, Improvement of Regulation of the entities of the Payment Service Market, Universal Declaration and Restoration of Economic Growth dated July 03, 2020 made amendments in the Law On Payments and Payment Systems related to identification of the customers of electronic money systems (EMS); prohibition to make payments and transfers to identified customers by unidentified customers; prohibition to pay or transfer electronic money owned by unidentified person to any EMS agent; limitations of transaction amount, total amount of daily transactions and maximum amount of electronic money kept in one wallet; prohibition to transfer electronic money through transfers to bank accounts or means of electronic payment of owner of electronic money that is natural person without confirmation that this person owns the bank account or the means of electronic payment.

237. Amendment in the Law On Microfinance Activities has been made that strengthens the requirements to microfinance organizations (MFOs); legal entities registered as MFOs should within six months contact the competent authority to obtain a license for microfinance activities; legal entity that intends to conduct activities to grant microloans should notify FMA of the registration/re-registration as MFOs within 10 calendar days from the date of registration; minimum authorized capital and shareholder equity of pawnshops in towns of republican significance and regional capitals have been gradually increased from 50 mln to 100 mln KZT, for other regions, from 25 mln to 50 mln KZT.

238. The assessors also concluded that the Republic of Kazakhstan pays high-level attention to AML/CFT issues. The Order of the President of the Republic of Kazakhstan confirms this; it introduced the "follow the money" principle in the activities of FMA and other law enforcement authorities' activities and implemented measures to recover funds siphoned abroad. In addition, law enforcement authorities implement this Order with respect to prioritization of the fight against ML/TF and strengthening efforts to conduct parallel financial investigations.

239. The measures taken indicate a significant reduction in criminal activity. The total number of crimes recorded in the URPI decreased by 50% in 2021 compared to 2017.

240. A similar trend can be seen for predicate offences. In particular, economic crimes (including tax crimes) in 2021 compared to 2017 decreased by 28.8%, corruption crimes - by 36.5%, and thefts by

misappropriation or embezzlement - by 65.9%. Illegal drug trafficking (article 297 of the CC) decreased by 22.6%, crimes related to the creation and management of organized criminal groups and participation in such groups (article 262 of the CC) by 73.6%, and the organization of illegal gambling business (article 307 of the CC) by 60.7%.

241. Representatives of the competent bodies explained that the main objective of the state criminal law policy is the prevention of crime. In this regard, the LEA/SSAs are focused on strengthening the preventive component in order to prevent the commission of crimes or to detect them at the stage of preparation to commit them.

242. Measures were taken to reduce the vulnerability of the banking sector. In particular, at the initiative of pre-trial investigative authorities, changes were made in the NB reporting, according to which STBs are required to provide monthly information on the amount of cash given out to legal persons. This information is analyzed by the prosecution authorities in accordance with the developed methodology to identify violations of the AML/CFT legislation by banks.

Case Study 1.1. Use of criminal case data for FIU purposes

In the criminal case against D., it was established that in 2019 two companies controlled by an organized criminal group in one of the branches of Bank A cashed out KZT 1.2 billion (more than USD 3.1 million) in 70 transactions. Despite the fact that 82% of transactions exceeded the threshold, the bank failed to inform the FIU. Based on the bank inspection results, the authorized body drafted five administrative protocols for violations of the AML/CFT legislation, and the guilty persons were held administratively liable. In 2020, cashing-out at this bank branch decreased 5 times.

243. In accordance with CPC Article 200, when the circumstances contributing to the commission of a criminal offence are established in the proceedings, the person conducting the pre-trial investigation has the right to make a requirement in respect of the elimination of violations of the law, which is subject to mandatory consideration with informing the pre-trial investigative authority on the measures taken. Between 2017 and 7 months of 2022, the EIS sent 76 statements on violations of the AML/CFT legislation in pending criminal cases to STBs, 8 - to the NB, and 14 - to the ARDFM. Based on the statements, 7 bank officers were brought to disciplinary responsibility and 3 officers were dismissed. For the rest of the statements, explanatory work and training of STBs officers were carried out.

244. The outcomes of TF NRA 2018 and 2021 made it possible to identify key threats, vulnerabilities and risks to the national system and determine the main directions of the national anti-terrorism policy, which are reflected in such normative acts as the National Security Strategy (approved by Presidential Decree in 2021), the State Programme on Countering Religious Extremism and Terrorism for 2018-2020, the Special Plan for Countering, Neutralizing and Eradicating Destructive Movements (2018), the Roadmap for Preventing and Avoiding the Spread of Destructive Religious Movements among Minors (2020), and the Complex of Systemic Measures for Countering Religious Extremism and Terrorism (2022), etc. The above documents define the strategic directions of counter-terrorism actors and their tactics, which include eliminating the financial basis of terrorism, preventing TF crimes, identifying sources of TF, suppressing the activities of terrorists, terrorist organizations and those who finance them.

2.2.3. Exceptions and application of enhanced and simplified measures

245. The NRA has not identified a need to apply enhanced measures; however, the MFOs' risk level has been revised. Also, following the NRA collectors have been removed from the list of obliged entities. All obliged entities should apply enhanced measures in high risk situations and may only apply simplified measures in low risk situations except for the cases prescribed by the AML/CFT law (for instance, when services to quasigovernment enterprises are provided).

246. Following the NRA, approaches to ICR have been revised. Now obliged entities' ICR include Risk Management Program that specifies the main risk criteria and enables to ensure the adequate monitoring of the transactions of obliged entities' customers for AML/CFT purposes. The obliged entities annually assess

the level of vulnerability of their services/ products to ML risks taking into account, as a minimum, the categories of risks such as the type of customers, country/geographical risk, the risk of service/product and/or a way to provide it. There are obliged entities and their customers that have, depending on their activities, increased and reduced ML risk.

247. The outcomes of the risk assessments are used to develop two categories of response measures: enhanced due diligence measures should be applied to customers, their representatives or beneficiary owners if the ML/TF risk is high; simplified due diligence measure should be applied to customers/their representatives and beneficiary owners if ML/TF risk is low

2.2.4. Law enforcement authorities' tasks and activities

248. The government authorities of Kazakhstan take into account the outcomes of the assessments to identify tasks and take measures. At operational level, government authorities have brought their policies, functions and priorities in compliance with the outcomes of risk assessments through development of plans. Taking into account the NRA outcomes, activities of the units of some government authorities have been reoriented. For instance, FMA has established new units to identify transactions involving PEPs and VA-related transactions. In addition, a new department has been established to examine obliged entities. Law enforcement unit of FMA has 18 investigative teams comprising 52 investigators that only conduct parallel financial investigations. MIA of the RK has a cyber security unit, Anti-Corruption Agency and the General Prosecutor's Office, an asset recovery unit. The activities of AML/CFT regulatory authorities comply with the requirements of the FATF Standards related to staffing, expertise and material and technical resources.

249. The central competent body in the field of combating terrorism and TF is the NSC, which has special units (Department for Combating International Terrorism, Investigation Department and others). The strategic directions of the NSC are defined by national acts and include measures to mitigate risks and suppress TF threats.

250. In addition, the NSC coordinates the activities of counter-terrorist agencies. For this purpose, the Anti-Terrorist Centre was established in RK and consists of the heads of 20 government authorities. The ATC is responsible for determining state policy, improving counter-terrorism legislation, developing practical measures for government authorities to improve their effectiveness in combating terrorism, forecasting terrorist threats and introducing international experience in the area of counter-terrorism. More than 200 counter-terrorism commissions under the executive authorities are coordinated by the Operational Headquarters for Combating Terrorism within the ATC.

2.2.5. National interaction and cooperation

251. Interaction and cooperation are one of the strengths of the Kazakh AML/CFT framework. FMA is responsible for steering and coordination of AML/CFT activities; it receives high-level support. One of the effective tools is Interagency Working Group on Preparation to the Second Round of Mutual Evaluation of EAG (the Working Group) established under the Executive Office of the President of the Republic of Kazakhstan. The Working Group is an advisory and consultative authority; it was established to developing measures to implement state policy in the sphere of AML/CFT and increasing their effectiveness, as well as coordinating measures aimed at reducing the risks of money laundering and terrorist financing and combating the shadow economy.

252. The Working Group comprises the officials of the Executive Office of the RK, Security Council of the RK, Supreme Court, the General Prosecutor' Office, Ministry of Foreign Affairs, National Security Committee, Ministry of Internal Affairs, FMA, Anti-Corruption Committee, ARDFM, APDC, NB, Audit Committee, Agency for Strategic Planning and Reforms, Ministry of National Economy, Ministry of Finance, Ministry of Health, Ministry of Education and Science, MCS, Ministry of Justice, Ministry of Digital Development, Innovations and Space Industry, Ministry of Transport and Integration, Ministry of Agriculture, Ministry of Information and Social Development, Ministry of Economy, Ministry of Industry and Infrastructure Development, Ministry of Ecology, Geology and Natural Resources, Atameken Research and Production Enterprise and AFSA.

253. Before September 2020, AML/CFT Interagency Commission operated in Kazakhstan. As part of preparation for mutual assessment of Financial Monitoring Committee of Ministry of Finance of the Republic of Kazakhstan (now FMA), energetic efforts were made to enhance the AML/CFT framework to reach compliance with the FATF Recommendations. In November 2020, provision of Article 11-1 of the AML/CFT Law became effective, under which the AML/CFT Interagency Board was established in Kazakhstan that became a forum to shape the AML/CFT/CPF government policy. It comprised deputy directors of law enforcement, special and regulatory authorities involved in AML/CFT/CPF. The Board is an advisory and consultative authority; it was established to develop measures to implement the AML/CFT/CPF government policy and enhance their efficiency, as well as to coordinate measures to mitigate the ML/TF/PF risks. Following the meetings of the Board, a number of documents has been approved, including guidelines to identify PEPs and beneficiary owners, and recommendations for the NPO sector. Based on the results of the meetings of the MIA on AML/CFT/FFTF issues, a number of strategically important documents were approved and adopted, including the closed and public versions of NRAs, sectoral assessment of NPOs, as well as the vulnerability report of legal entities, methodological recommendations for identifying PEPs, beneficial owners and approved recommendations for NPOs in the field of FTF.

254. To enhance interaction with FMA and solve organizational and legal issues, in November 2019 the Compliance Board under FMA was established. The main tasks of the Board are to prepare recommendations to implement new forms of interaction with and feedback for FMA; prepare and discuss proposals to improve information sharing between FMA and the Agency as well as on other communication issues; participate in the projects related to notification of obliged entities of ML/TF risks to be used to implement internal control procedures; arrange and participate in joint training events, exchange AML/CFT best practices and experience, including with the involvement of visiting experts. From the launch of this forum, over 70 meetings with obliged entities and government authorities have been held, where, for instance, unified register of high-risk persons and the findings of ML/TF/PF NRA, etc. were discussed.

255. Cooperation and information sharing agreements, action plans of FMA and other government authorities prescribe other elements of AML/CFT interagency interaction. In addition, the action plans envisage a number of joint awareness raising events related to obliged entities' compliance with AML/CFT laws, application of the criteria of assessment of risk levels, identification and review of risks, development of measures to mitigate the identified risks, development of recommendations and guidelines to assess the risks. Over 10 AML/CFT cooperation and interaction agreements and joint orders have been signed with each regulatory authority, under which government authorities on an ongoing basis share information on the obliged entities that have data to comply with the AML/CFT Law, as well as to involve in AML framework; also, 31 agreements with public organizations have been signed. 39 AML/CFT interaction memoranda have been concluded with foreign FIUs; also, 10 agreements between Economic Investigation Service and foreign competent authorities have been concluded. For instance, agreement with Ministry of Information and Social Development (interaction on NPO activities) and joint order approved by FMA, NSC and SRC of Ministry of Finance on interaction to share and transfer ML/TF/PF information, data and documents to combat illegal movement of cash and/or money instruments have been signed.

256. The Working Group on Implementation of the Pilot Project on the Activities of Crypto-exchanges under AFSA approved by the Order of MDD No. 207/NK dated June 11, 2021 comprises AFSA officials. Also, AFSA officials are the members of the Interagency Working Group on Development of Measures to Combat Ponzi Schemes approved by the Order of the Chairman of ARDFM No. 388 dated October 7, 2020.

257. Law enforcement and special authorities properly maintain interagency interaction. Interagency AML/CFT interaction is conducted under a Joint Order On Approval of Guidelines of Interaction to Share Information, Data and Documents between Law Enforcement/Special Authorities and FMA that regulates all necessary issues: prompt processing of requests; form of notification of FMA when law enforcement/ special authorities identify suspicious transactions; prosecutor office's powers to authorize requests; authorized request form with special marks; procedure for removal from TF list before a criminal record is expunged; procedure for payments to the persons from the TF List (wages, insurance and tax payments,

penalties, state fees, travel allowances, pensions, scholarships and other social benefits). The evaluators highlight effective interaction between NSC and other appropriate government authorities, including as part of international cooperation in the course of humanitarian operation Zhusan when Kazakh nationals (women and children) were evacuated to Kazakhstan from Syria. Kazakhstan has established Interagency Center for Coordination of the Activities of Government Authorities to Combat Drug Addiction and Drug Trafficking[11]. ARIN-WCA comprises the officials of the General Prosecutor's Office of RK and Investigative Committee of Ministry of Internal Affairs of the RK.

258. In 2018, Interagency Investigative Team (IIT) under the General Prosecutor's Office of RK was established. It comprised the officials of the General Prosecutor's Office, Anti-Corruption Agency, Ministry of Internal Affair and FMA. For the last 5 years, prosecution authorities established over 50 IITs, Also, Anti-Corruption Agency and its regional units established approx. 20 IITs that comprise the officials of MIA, FMA and NSC.

2.2.6. The private sector's risk awareness

259. FIs and DNFBPs that should follow AML/CFT requirements were directly involved in national and sectoral risk assessments. In particular, during preparation for the 2018 and 2021 ML/TF national risk assessments surveying was conducted. The survey covered all concerned government authorities and a large part of the private sector. In the course of the NRA, the Compliance Board conducted consultations with the public and the private sectors. These consultations were conducted to discuss and identify trends, risks and their opinions on the measures to mitigate risks.

260. The findings of the risk assessments were properly communicated to the President of the Republic of Kazakhstan and his Executive Office, as well as government and law enforcement authorities. The risk assessments were also communicated to FIs, DNFBPs, VASPs, NPOs and SRBs through their accounts on FMA's web-site and during bilateral and multilateral meetings, conferences and other events.

261. All competent authorities and SRBs published on their web-sites public versions of the reports on the national ML/TF/PF risk assessment. Clause 6, Article 11-1 of the AML/CFT Law requires from obliged entities to take into consideration the published information from risk assessment report when they implement the programs included in internal control guidelines. Supervisory authorities recommend the private sector to take into account and use the findings of the national and sectoral risk assessments to identify, assess, manage and mitigate risks.

262. Reporting entities freely and without any problems discussed with the evaluators the findings of the national and sectoral risk assessments and the existing threats, vulnerabilities and risks related to their activities.

Overall conclusions on Immediate Outcome 1

263. The Republic of Kazakhstan makes considerable efforts to identify, understand and assess the national ML/TF risks and develop measures to mitigate them. Despite the fact that the ML NRA has no finding on the specific ML risks, the approach used to assess the predicate offences that generate main proceeds and review ML-related criminal cases reflects the needs of the country. In turn, the TF/PF NRA clearly specifies inherent TF risks. The national AML/CFT policy is shaped on an ongoing basis and is properly aimed at mitigating the identified ML/TF risks. The findings of the risk assessments were adequately taken into account to identify the tasks and measures to be accomplished and taken by competent authorities. The findings of risk assessments are communicated to FIs, DNFBPs, VASPs and SRBs through institutional and operational mechanisms. In general, the members of the AML/CFT framework (both the public and the private sectors) have demonstrated understanding of ML/TF risks. However, the evaluators highlight that there is scope to further improve the methodology of ML risk assessment, enhance understanding of inherent risks and use the NRA findings to develop comprehensive interagency plans to mitigate the identified risks.

[11] Order of the Prime-Minister of the Republic of Kazakhstan No. 129-r dated September 15, 2011

264. **Kazakhstan is rated as having a substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. All LEAs/SSAs regularly and effectively obtain and use financial intelligence and other relevant information to gather evidence for investigations of money laundering, terrorist financing and predicate offences and tracing criminal proceeds. Information may be obtained either independently or through the FIU.

2. All LEAs/SSAs, namely the FMA's own operational and investigative units actively request information from the FIU regarding high-risk predicate offenses (except for illegal economic activity and drug trafficking) and ML, while information on combating TF is less actively requested by relevant competent authorities, while FMA's sending of proactive materials on TF tends to decrease. The MIA and the AIC made less use of the FIU's ability to obtain relevant financial information as part of international cooperation.

3. The FIU has a vast amount of data at its disposal, including a large number of suspicious transaction reports and reports of transactions subject to mandatory monitoring. The FIU uses state-of-the-art technology and a high level of process automation to prioritize, initiate and facilitate investigations conducted by LEAs/SSAs.

4. The information contained in the FIU database is used to assist ongoing investigations, as well as to initiate new investigations into predicate offences and, less frequently, money laundering (except the EIS) and terrorist financing. Case studies and statistics show that analysis data are used to investigate cases that are proactively referred to law enforcement authorities as well as to assist ongoing investigations.

5. LEAs/SSAs have also demonstrated that financial investigation data communicated proactively or upon request is of high quality and an inseparable part of their work.

6. Most threshold and suspicious transaction reports are received by the FIU from financial institutions; DNFBPs submit them in smaller numbers. The FIU also receives other additional information from STBs upon request. Besides that, the FMA also receives information on transactions suspended by the obliged entities prior to their conduct due to suspicion of ML/TF.

7. The FIU has excellent resources and information capabilities and competent analysts who have in-depth knowledge of the national AML/CFT system specificities.

8. AML/CFT cooperation at the national level is a strength of the Kazakh AML/CFT system. LEAs/SSAs noted the close cooperation and effective coordination on ML/TF issues, for which purpose separate dedicated platforms were established to determine the directions of state policy in this area. The exchange of information between the FMA and the RK competent authorities is carried out exclusively via secure communication channels.

Immediate Outcome 7

1. Kazakhstan has demonstrated successful exercise by LEAs/SSAs of their powers of detecting money laundering and prosecuting these offences. Most ML offences are committed in the form of self-laundering (through the acquisition by natural persons of movable and immovable property with criminally obtained funds and its fictitious registration in the ownership of third parties, the introduction of legal persons into the economic turnover under the guise of legally acquired production equipment and immovable property objects), but there have also been prosecutions and convictions for ML by third parties, including professional money laundering. There was no conviction for stand-alone money laundering.

2. A unified methodology for conducting parallel financial investigations is defined for the LEA/SSAs, and access to a wide range of information on individuals and legal entities, including financial information, is ensured. Special structural subdivisions have been established in the EIS and ACA, whose competence includes solely the implementation of parallel financial investigations. The promptness of criminal prosecution is facilitated by the introduced form of pre-trial investigation in electronic format through the "Electronic Criminal Case" module,

3. In addition to financial investigation subdivisions, all LEAs/SSAs also established specialized analytical units that provide information and analytical support for the activities of operational and investigative units, including analytical identification of criminal schemes for predicate offences, development of ML typologies, preventive measures, proposals to enhance the effectiveness of interagency cooperation and improve legislation.

4. The level of interagency cooperation between LEAs/SSAs is high. LEAs/SSAs use MLA mechanisms and other forms of international cooperation to fulfil their criminal prosecution tasks.

5. The country pays significant attention to ensuring the availability of highly qualified staff in LEAs/SSAs and the judiciary. The competent authorities have the necessary human, information and analytical resources.

6. There are no aspects of the investigative, prosecutorial, or judicial process that impede or hinder the prosecution and sanctioning of ML.

7. The prosecution for ML is generally consistent with the nature of national threats and risks and national AML policies, with the exception of crimes in the field of illicit drug trafficking, the detection of facts of ML for which is insignificant, as well as of theft, as the ML threat level that it poses was not determined during the NRA.

8. Sanctions for ML offences against natural persons are proportionate, dissuasive and effective. No sanctions were applied to legal persons for ML offences.

9. If ML is not proved, criminal prosecution and conviction for the predicate offence are carried out, and if a conviction for ML cannot be secured due to search, death, amnesty of person or expiry of the statute of limitations, the pre-trial confiscation of criminal property is applied.

Immediate Outcome 8

1. Confiscation of criminal proceeds, instrumentalities of crime and property of equivalent value is considered as a consequence of committing a criminal offence and is a means of implementing the state criminal law policy in the sphere of combating crime.

2. Confiscation of criminal proceeds, instrumentalities of crime and property of equivalent value under the RK criminal law is an additional punishment and is imposed by a court sentence in those cases where it is provided for by the sanction of the CC article. Besides that, confiscation of illegally obtained property is applied prior to sentencing as a measure under criminal law on the basis of a court decision in cases prescribed by law.

3. During the CIDA and pre-trial investigations, pre-trial investigative authorities conduct parallel financial investigations in order to find property subject to seizure. The effectiveness of parallel financial investigations is enhanced by special units established within the EIS and ACA, which are exclusively responsible for such investigations.

4. The courts apply confiscation of the proceeds of crime, property acquired by criminal means, instrumentalities and means of crime, and property of equivalent value.

5. Comprehensive statistical records are not maintained, in particular, statistics on the amount of criminal proceeds from predicate offences, types of confiscation, separate records on the valuation and sale of property confiscated on criminal, administrative or other grounds.

6. Customs authorities are not LEAs per se, but they carry out activities on detecting, preventing and suppressing criminal and administrative offences in the field of customs legislation. At the same time, they are significantly limited in their powers and access to information resources compared with LEAs/SSAs.

7. Confiscation of undeclared (falsely declared) cash is not effective, proportionate and dissuasive and does not contribute to the suppression of cash couriers' activities.

8. It was not possible to draw conclusions about the consistency (inconsistency) of confiscation with the ML/TF risk assessment.

Recommended Actions

Immediate Outcome 6

1. The NSC, ACA and MIA should make greater use of the FIU resources and capabilities to obtain financial intelligence and other information as they investigate the financial aspects of predicate offences and identify the fact of ML itself.

2. All LEAs/SSAs should continue to use financial analysis and other relevant information to better identify illegal economic activity and illicit drug trafficking in accordance with the risks specified in the ML NRA report, as well as pay particular attention to identifying the facts of laundering of proceeds derived from these categories of crime.

3. The RK competent authorities engaged in combating terrorism and its financing should actively request financial intelligence and other information from the FIU when conducting police intelligence operations or investigations into terrorist offences.

4. The MIA and ACA should actively use the FIU capabilities to obtain significant financial intelligence as part of the FIU international cooperation for tracing criminal proceeds and determining the extent of cross-border offences within the purview of these authorities.

5. The FMA should pay more attention to the analysis, preparation and proactive submitting of TF-related materials, if it is necessary to involve the relevant competent authorities to determine the priority areas of analytical activities for improving the quality of use and feasibility of the FIU analysis results in practice.

Immediate Outcome 7

1. Kazakhstan should analyze the reasons for the lack of successful prosecutions for ML without a predicate offence, with the adoption of legislative regulation if necessary.

2. The competent authorities should ensure the effectiveness of parallel investigations according to the established single methodology. The MIA and NSC should consider creating special structural subdivisions or allocating individual officers, whose competence will include only conducting parallel financial investigations.

3. It would be useful to intensify the work of the ACA to identify ML from corruption crimes, and the MIA - from crimes in the sphere of illicit drug trafficking.

4. In order to further improve the effectiveness of sanctions for ML against natural persons it would be useful to perfect the practice of sentencing. The final punishment for ML combined with a predicate offence, as a rule, should be imposed taking into account the public danger of ML (by the addition of penalties).

5. Ensure the practical implementation of bringing legal persons to administrative liability for ML. Consider expanding the range of sanctions against legal persons.

6. It is necessary to adjust approaches to the maintenance of statistical records, to provide for the recording of ML offences with reference to predicate offences at all stages of the criminal process.

7. Continue the practice of international cooperation to identify the facts of the transfer of criminal assets abroad, including ML in foreign jurisdictions and ML in the country when committing a predicate offence abroad.

Immediate Outcome 8

1. The Republic of Kazakhstan should consider amending legislation to expand the institution of pre-trial confiscation of criminal property, instrumentalities and means of crime in criminal cases, as well as the possible introduction of the institution of non-conviction based confiscation of the incomes from unconfirmed sources.

2. Pre-trial investigative authorities should intensify activities on identifying property subject to seizure, including transferred to foreign jurisdictions and taking provisional measures for the subsequent confiscation of property and criminal injury compensation, as well as recovery of criminal assets from foreign jurisdictions.

3. The compulsory enforcement authorities should take additional measures to improve the effectiveness of the actual execution of court decisions on the recovery of property damage and forfeiture to the state.

4. GPO approaches to keeping statistical records should be adjusted. For these purposes, it is necessary to provide for the reflection in the criminal statistics of the amount of income from predicate offences and the types of seized property. It is necessary to unify the statistics of the pre-trial investigative agencies, courts and compulsory enforcement authorities to be able to compare the amount of seized property, property confiscated by courts or converted into compensation for damages and the actual execution of court decisions on all ML and predicate offences.

5. Approaches to customs administration should be revised. To improve the efficiency of customs authorities, consideration should be given to expanding their powers (in particular, by granting direct access to the Law Enforcement and Special Agencies Information Exchange System), as well as automating the profiling system and other means of implementing customs control measures.

6. To ensure the effectiveness of measures aimed at disrupting cash couriers' activities, it is necessary to adjust national legislation to introduce confiscation as a measure of administrative liability for non-declaration (false declaration) of cash and refer cases of administrative offences of this category to court jurisdiction.

265. The relevant Immediate Outcomes considered and assessed in this chapter are Immediate Outcomes 6, 7 and 8. Recommendations 1, 3, 4, 29 - 32 and also elements of R.2, 8, 9, 15, 30, 31, 34, 37, 39 and 40 are used in assessing effectiveness in this section.

3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

3.2.1. Use of financial intelligence and other relevant information

266. All LEAs/SSAs of Kazakhstan, including the EIS, MIA, NSC, ACA and GPO, regularly and effectively use financial intelligence and other relevant information to gather evidence for investigating ML, TF and predicate offences, as well as for tracing criminal proceeds. All LEAs/SSAs have ample opportunity to obtain relevant information independently, including bank secrecy, directly from financial institutions after a criminal case is registered in the Uniform Register of Pre-Trial Investigations (UPRI)[12].

267. LEAs/SSOs are not entitled to obtain information that constitutes a banking secret (see R.31.3(a)) at the stage of criminal prosecution (i.e. prior to registration in the UPRI). However, it is possible to obtain such information through the FIU.

[12] The UPRI is an automated database that records information on criminal reports, related procedural decisions, actions taken, the progress of criminal proceedings, applicants and participants in criminal proceedings.

268. LEAs/SSAs use a variety of information resources, primarily the Law Enforcement and Special Authorities Information Exchange System (LESA IES). The system is used to obtain information in criminal, civil, administrative, search and enforcement proceedings. The system is integrated with 81 information databases of 26 authorized bodies and government authorities, 21 STBs:

- information on natural persons and identity documents, residence addresses, next of kin, dispensary registration, crossing the state border by Kazakh and foreign nationals;
- information on entrepreneurial activities of natural persons, individual entrepreneurs, legal persons, on public procurement, importers/exporters;
- information on immovable property objects and ownership of objects, availability or non-availability of ownership rights to land, vehicles registered with the internal affairs authorities;
- tax and customs[13] information;
- databases of persons held criminally and administratively liable; and other information.

269. LEAs/SSAs also receive financial intelligence and relevant information from foreign partners through Interpol, other relevant operational/industry associations and as part of MLA (see Chapter 8).

270. LEAs/SSAs have access to the FIU information (provided both upon request and proactively). The FIU is a core element of the national AML/CFT regime in Kazakhstan. The FMA maintains a national AML/CFT database (Unified Information and Analytical System, UIAS) that contains all threshold and suspicious transaction reports, transactions of designated persons, transactions with characteristics consistent with ML/TF typologies, schemes and methods, reports of refusals to establish business relationships, refusals to conduct transactions and termination of business relationships, as well as information received from the obliged entities on additional requests. The content of this database is also supplemented by information on suspicious transactions and/or activities of legal and natural persons received from the RK government and law enforcement authorities, as well as from FIUs of foreign countries.

271. In addition to approximately 2 million threshold and suspicious transaction reports received from the obliged entities each year and contained in the national AML/CFT database, the FMA also uses other financial and non-financial information from other Kazakh ministries and agencies through automated access when conducting financial investigations (see Table 6.1). Besides that, the FIU uses information obtained through international cooperation, as well as from open sources (social networks, messengers), and for the latter, modern software products have been developed to obtain relevant information.

Table 6.1. List of information accessible to FMA

No.	IS	Beneficiary	Information content
1.	Integrated Tax Information System	SRC	Information on the availability of bank accounts, about owners, managers, founders, type of activity, budget payments, personal accounts, etc.
2.	IS Berkut	NSC	Data on state border crossings, information on encumbrances on border crossings
3.	Information System of the Committee on Legal Statistics and Special Accounts of the GPO	Committee on Legal Statistics and Special Accounts of the GPO	Information on criminal and administrative offences
4.	Tax Reporting Processing System	SRC	Information on tax returns, declarations, calculations, register of accruals
5.	WEB portal of public procurement		Information on electronic services in public procurement

[13] The Agency has online access to the information system of the customs authority "Astana-1" (through the Oracle BI report designer), through which it is possible to upload passenger customs declarations (PTD) as per the list of persons (or other criteria: country, date, amount and etc.), as well as the entire data array.

6.	Law Enforcement and Special Authorities Information Exchange System	GPO	81 information services of more than 26 government authorities and organizations (Ministry of Justice, NSC, MIA, SRC, Ministry of Economy, Ministry of Agriculture, Transport Committee, Ministry of Health, etc.).
7.	FMA URPI	Committee on Legal Statistics and Special Accounts of the GPO	Information on pre-trial investigations, criminal statistics data, analytics modules, records of persons taken to LEAs/SSSs' buildings, operational summary of the LEAs/SSSs information, Crime Record Book data, etc.
8.	Web URPI	Committee on Legal Statistics and Special Accounts of the GPO	Electronic criminal proceedings, pre-trial investigations data, requests for medical records (psycho/narcotics), online authorization of restrictive measures, restrictions on immovable property, imposing a ban on crossing the state border, etc.
9.	Customs Automated Information System (TAIS-2) Information System on Reception and Processing of E-Invoices (EI IS) "Unified Data Repository" Information System (UDR IS) "Astana-1" IS	SRC	Information on customs procedures and operations Information on electronic invoices Information on the owners, heads, founders, type of activity, budget payments, personal accounts Information on customs procedures and operations.

272. LEAs/SSAs, including the EIS, based on the Joint Agreement (No. 1009-dsp dated October 14, 2020), submit to the FIU prosecutor-approved requests for financial information, including from foreign partners, when conducting parallel financial investigations, investigations of predicate offences and ML/TF. The information received from the FIU is used to gather evidence both at the Police Intelligence Operations stage and in criminal proceedings. According to the information received during the on-site mission, in practice, warrants are obtained from 1 to 3 days, and in case of urgent need - within a few hours. There were no refusals to obtain warrants.

Table 6.2. Number of requests for financial intelligence sent to FMA by LEAs/SSAs

LEAs/SSAs	2017		2018		2019		2020		2021		1st half of 2022		2017-2022	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
EIS	60		10		5		6		40		110		231	
NSC	1		3	1	8		10	2	14		2		38	3
MIA	2		3	2	5	2	23	19	14	5	13	1	60	29
ACA	24		18		9		20		10		3		84	
GPO	28		39	3	19	1	29	1	0		8	2	123	7
TOTAL	**115**		**73**	**6**	**46**	**3**	**88**	**22**	**78**	**5**	**136**	**3**	**536**	**39**

273. An analysis of the inquiries received by the FA through ML shows that 41.7% of such inquiries came from LEAss/SSA as part of their investigation of tax crimes, 27.8% - embezzlement of budget funds and corruption, 17.3% - fraud, incl. financial pyramids, 4.4% - illegal economic activity and 8.6% - other predicate crimes.

274. As shown in the table above, LEAs/SSAs, specifically the EIS, actively request information from the FIU regarding high-risk predicate and ML offences.

Case Study 6.1. Information sent by FMA on the request of EIS

In 2017, on the initiative of the EIS, the FIU revealed suspicious transactions on P B LLP in the territory of Almaty.

Obliged entities) received 107 reports of threshold and suspicious transactions in relation to P B LLP, including replenishment of the account and account, as well as withdrawal from the account .

The main operations are related to the systematic replenishment of the account in cash and withdrawals from the account of cash as a withdrawal of winnings. And also there was information on account replenishment through the payment system of QIWI Kazakhstan LLP.

At the same time, as part of the analysis, it became known that there was negative information about the recovery of a debt by a private enforcement agent in favor of an individual.

The FIU sent the relevant information to the territorial department of EIS.

07.10.2017 EIS in relation to "O" and other persons, pre-trial proceedings have been initiated on the fact of organizing a network of illegal gambling establishments in the bookmaker offices of "P B" LLP, in order to generate income on an especially large scale in the amount of more than 5.3 billion KZT.

Criminal proceeds from the activities of illegal gambling in the amount of more than 5 billion KZT were transferred through payment terminals to bank accounts opened in the name of "O", "V" and their close relatives. Further, “O” and “B”, in order to legalize criminal proceeds from illegal gambling, acquired expensive real estate (parking space) and movable property (elite cars of 5 brands with a total value of over 200 million KZT).

The specified property and bank accounts of the defendants in the case (580.2 million KZT) were also seized with the court's sanction.

By the verdict of the Almaly District Court of Almaty dated 05/20/2021 "O" and "O". convicted under Article 307, Part 3 (illegal gambling business), Article 218, Part 3, Clause 3 of the Criminal Code (money laundering), with a sentence of 4 years in prison, with confiscation of criminal proceeds and property obtained by criminal means in the amount of more than 780 million KZT.

275. LEAs/SSAs request from the FIU financial intelligence (571 cases), beneficial ownership identification (150 cases) and asset tracing (150 cases), which proves that LEAs/SSAs are aware of the FIU's ability to handle information, including bank secrecy.

276. In terms of combating TF, the bulk (71%) of the FIU interaction is with the NSC, which is the coordinating and competent authority for combating terrorism and its financing. However, the TF information exchange tends to decrease, i.e., in 2018 they prepared and sent to the competent authorities 107 proactive materials, in 2019 - 57, in 2020 - 21 and in 2021 – 11, Thus, if in 2018 107 initiative materials were prepared and sent to the competent authorities, then in 2019 - 57, in 2020 - 21 and in 2021 - 11 materials were sent on an initiative basis.

Case Study 6.2. Provision of information by FMA at the request of NSC

In 2017, the FIU, at the initiative of the NSC, conducted an investigation with regard to individual E. N. and terrorist financing, which also involved the use of reports received from obliged entities.

E.N. is a relative of designated individual A.E. Individual E.N. received money from third parties on a gratuitous basis and then repeatedly sent funds through the "Western Union" money transfer service to the addressee in Germany (KZT 1,543,579 was received between March 11, 2015 and September 26, 2016). Multiple transfers of individual E.N. came into view, who made 13 replenishment transactions between March 2015 and April 2016 for a total amount of KZT 4,928,000. In total, E.N. conducted 400 transactions to the amount of more than USD 10 thousand.

The results of the FIU's financial monitoring allowed law enforcement authorities to establish and confirm speculation that individual E.N. is actively involved in terrorist financing and supports the ideology of destructive religious movements.

As a result, on January 4, 2018, the District Court No. 2 of the Saryarka District of Astana found individual E.N. guilty of committing a terrorist offence and sentenced to imprisonment for a term of 6 years under CC Article 258(1).

277. Based on the results of the FIU's analytical activities, when indicators of predicate offences and ML/TF are identified, analysis results are proactively forwarded to the EIS and other LEAs/SSAs, which are the authorized agencies that detect and investigate these offences.

Table 6.3. Statistics of proactively submitted FIU materials broken down by recipient

LEAs/SSAs	2017		2018		2019		2020		2021		1st half of 2022		2017-2022	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
EIS	77	16	90	31	109	11	106	4	169	2	50	3	601	67
NSC	9	41	15	73	11	42	10	17	8	9	4	11	57	193
MIA	3	2	7	3	13	4	43		37		13	2	116	11
ACA	8		5		9		1		17		3		43	
TOTAL	**97**	**59**	**117**	**107**	**142**	**57**	**160**	**21**	**231**	**11**	**70**	**16**	**817**	**271**

278. As the table shows, the FIU provides proactive ML materials primarily to its operational investigative unit (61%), since the EIS detects and investigates most of the predicate offences that pose the highest ML risk, and according to the NRA, these categories of crime have the highest criminal income and amount of damage caused. Besides that, nearly 12% of the FIU's proactive materials related to drug trafficking and fraud were sent to the MIA for conducting relevant CIDA.

279. However, the ratio of information sent upon request and proactively may suggest that the need for obtaining a warrant limits LEAs/SSAs and, above all, the EIS to a small extent.

280. The effectiveness of the use of FIU materials tends to increase, if in 2017 LEAs/SSAs used 38% of FIU materials, in 2021 this figure was 64%. All the FIU materials received upon request were used by the LEAs/SSAs in the initiation of criminal proceedings, confirmation of information already held by the initiators of the request, identification of other persons involved in the investigation, etc. The effectiveness of the use of FIU initiative materials by the LEAs/SSAs is 39%, with the greatest effectiveness is demonstrated in the implementation of these materials by the operative-investigative unit of the FMA, having used 50% of the FIU initiative materials in the course of investigation activities and investigative actions. Initiative materials sent to NSC and MIA were confirmed by them in 19% and 32% of cases, respectively.

Table 6.4. Effectiveness of the use of FIU materials by LEAs/SSAs

FIU materials	2017 г.	2018 г.	2019 г.	2020 г.	2021 г.	1-п. 2022 г.	TOTAL
Initiative	57 (37%)	60 (24%)	56 (27%)	88 (45%)	153 (60%)	39 (42%0	453 (39%)
Suspended transactions	184 (27%)	214 (43%)	312 (45%)	146 (42%)	162 (58%)	70 (37%)	1088 (40%)
By request	115 (100%)	79 (100%)	49 (100%)	110 (100%)	83 (100%)	139 (100%)	575 (100%)
TOTAL	**356 (38%)**	**353 (42%)**	**417 (44%)**	**344 (53%)**	**398 (64%)**	**248 (59%)**	**2116 (48%)**

281. As Table 6.4 shows, the FIU materials received by the LEAs/SSAs upon request were used in full, and the effectiveness of the use of initiative materials of the FIU for the assessment period is 39% and tends to increase from 2020, which, according to experts, the competent authorities effectively use initiative materials of the FIU.

282. Information received from the FIU was often used by LEAs/SSAs to gather evidence for such predicate crimes as tax crimes - 61%, embezzlement and corruption - 14%, fraud, including pyramid schemes - 14%, which are assigned a high risk by the NRA of 2021. However, the effectiveness of using FIU materials on illegal economic activity and drug trafficking, which are also assigned a high ML risk, is 1-2 % of the total amount of used/useful materials.

283. During the assessed period, 33% of criminal cases (112 out of 342) on money laundering (Article 218 of the Criminal Code of the Republic of Kazakhstan) were initiated on the basis of the FIU materials, provided both on a proactive basis and upon request. As noted above, the main volume of information exchange of the FIU falls on the financial investigation units of the FMA which initiated and investigated 89 (out of 112) criminal cases using the materials of the FIU.

284. It was also demonstrated to the experts that other LEAs/SSAs actively use the FIU materials. Out of 398 materials sent to the ACA, NSC the MIA, 266 were used in the course of investigative actions, mainly for predicate offences. Also with the use of materials of the FIU criminal cases were initiated and investigated for ML

Table 6.5. Percentage of criminal cases under ML and FT, initiated on the basis of FIU information

Cases involving ML and TF	**2017 г.**	**2018 г.**	**2019 г.**	**2020 г.**	**2021 г.**	**1-п. 2022 г.**	**TOTAL**
ML investigation using FIU information	**28**	**18**	**19**	**11**	**24**	**12**	**112**
ML investigation TOTAL	86	64	49	40	62	41	342
TF investigation using FIU information	**3**	**3**	**1**	**1**	**1**	**1**	**10**
TF investigation TOTAL	13	9	1	8	6	2	39

285. The analytical materials of the FIU on terrorism financing are also in demand by LEAs/SSAs. While 78 materials of the FIU were used by the NSC in conducting criminal investigations on terrorism financing cases, 10 criminal cases related to terrorism financing were initiated based on the FIU information, which is 26 % of the total number of criminal cases initiated in the country. The FIU strength is also the exercise of special control over the initiative materials sent to the own investigatiove units, which increases the effectiveness of their use.

286. Despite the FIU's significant contribution to detecting high-risk predicate crimes and ML in the country, and the focus on using financial information to detect these, it appears that other LEAs/SSAa are paying less attention to the need to use financial and other operational information to detect ML in predicate crime investigations.

287. The number of initiated cases on terrorism financing with the use of FIU materials decreases every year and in recent years this indicator is one case per year. The decrease in this number is probably due to a decrease in the number of initiative materials sent by the FIU on terrorism financing to the competent authorities (Table 6.3). In addition, if we take into account the number of criminal cases on terrorism-related crimes, which exceeds 600, and 39 LEAs/SSAs requests sent to the FIU under the TF for the entire evaluation period, we can conclude that the competent authorities in combating terrorism and its financing did not use FIU resources enough, and FIU initiative materials in this line did not fully meet the needs of these authorities.

3.2.2. Suspicious transaction reports received and requested by competent authorities

288. The FIU receives from FIs and DNFBPs a large number of suspicious transaction reports and reports of transactions with funds and/or other assets that are subject to financial monitoring. Suspicious transactions are subject to financial monitoring, regardless of the form they take and the amount for which they are or may be conducted.

289. The obliged entities send reports via secure communication channels and through a personal account on the FMA website exclusively using the approved FM-1 form, which consists of 4 sections: information on the data form and information on the transaction that is subject to financial monitoring, information on the obliged entities that submitted the FM-1 form, information on the transaction that is subject to financial monitoring and information on the participants in the transaction that is subject to financial monitoring. The FM-1 form contains information on one transaction, as well as on no more than two participants (payer

and recipient of the transaction).

Table 6.6. Statistics of threshold and suspicious transaction reports received

Report	2017	2018	2019	2020	2021	1st half of 2022	TOTAL
Threshold transactions	773 544	1 002 642	1 096 017	1 169 288	1 441 652	764 314	6 229 457
FIs	770 101	1 000 313	1 093 771	1 166 872			
DNFBPs	3 443	2 329	2 246	2 416			
Suspicious transactions	1 155 275	1 154 821	868 581	852 126	522 891	154 415	4 708 109
FIs	1 132 927	1 133 129	858 837	845 459			
DNFBPs	22 348	21 692	9 744	6 667			
TOTAL	1 928 819	2 157 463	1 964 598	2 021 414	1 964 543	900 729	10 937 566

290. In the assessed period, the FIU received nearly 11 million threshold and suspicious transaction reports from the obliged entities (an average of 5,000 each day), with 99% of these coming from credit institutions (see IO.4).

291. According to Table 6.4, there is a trend of almost halving the number of suspicious transaction reports from 1.1 million in 2017 to 0.5 million in 2021. The experts concluded that such trend is due to the measures taken by the FIU to improve the quality of the obliged entities' risk management systems, as well as the ongoing updating and optimizing the suspiciousness criteria, where special emphasis is placed on the quality of reports, and gradual reorientation towards reports that comply with the typologies and schemes developed by the FIU.

292. In particular, in order to improve the quality of reports received and the analytical component of the obliged entities, in 2017-2022, the FIU developed and disseminated to all types of them 57 ML/TF and predicate offence typologies, which provide for certain indicators of suspicious transactions conducted or being conducted by their customers.

293. The gradual improvement in the quality of suspicious transaction reports is also confirmed by statistics on such reports provided by the FIU in the context of suspicious transaction codes, where 45% of the total number of suspicious transactions in the assessed period (2,131,586 out of 4,708,109) were received with the following indicators identified by the obliged entities' primary analysis:

- clients, their activities, transactions or attempts to conduct them recognized as suspicious in accordance with the internal procedures of an obliged entity (code 7006 - 21% of the total number of suspicious transactions);
- transactions recognized as suspicious by the obliged entity officials according to their experience and knowledge (code 1036 - 14.5 %);
- withdrawal or transfer of all or a significant part of the money from a bank account within a short period of time after its crediting (code 4003 - 9.5 %).

294. The FIU, when preparing proactive materials or considering requests from LEAs/SSSs, actively uses both those received from the obliged entities and those processed through its STR databases, so that the FIU materials contain information received from financial institutions and are supplemented with evidence of suspicious activity and ML/TF and predicate offences.

Table 6.7. Statistics of reports used in the preparation of materials to be submitted to LEAs/SSAs

Year	**Number of submitted materials**	**Number of usedreports when submitting materials to LEAs/SSAs**			**Number of legal and natural persons analyzed in the preparation of materials**		
		Total	**Suspicious**	**Threshold**	**Total**	**Natural persons**	**Legal persons**
2017	**941**	**298 124**	173 294	124 830	**4 819**	2 880	1 939

2018	**834**	**396 662**	266 092	130 570	**4 516**	3 177	1 339
2019	**957**	**246 994**	103 412	143 582	**5 272**	3 935	1 337
2020	**654**	**195 859**	69 762	126 097	**4 928**	3 195	1 733
2021	**618**	**527 299**	312 677	214 622	**13 078**	9 753	3 325
6 мес. 2022	419	370 742	233 109	137 633	**6 518**	5 885	633
TOTAL	**4 423**	**2 035 680**	**1 158 346**	**877 334**	**39 131**	**28 825**	**10 306**

295. When conducting a financial investigation, STRs are used as basic information. Approximately 20% of the received reports served as the basis for the FIU's financial investigation or confirmed the suspicion and correctness of the law enforcement authorities' verification of persons against whom the FIU already had reports on their suspicious transactions.

Case Study 6.3. Use of suspended transactions by LEAs/SSAs

On June 4, 2021, information in relation to individual D was received from "Kaspi Bank" JSC on suspended suspicious transaction.

Individual D did not work anywhere, had a large turnover of funds in the accounts, reaching more than KZT 130 million. The money was transferred for participation in "Thefiniko" company, which, according to open information sources, raised money from individuals and had clear indicators of a pyramid scheme. The FMA decided to suspend this suspicious transaction and the relevant information was sent to the EIS for verification.

As a result of well-coordinated actions of the EIS, activities of the "Thefiniko" cross-border financial pyramid, which was a simulation of imaginary trading on world exchanges and attracted depositors as investors with the promise of huge returns (in the amount of 360-438% of invested funds) were suppressed.

The amount of funds raised was almost USD 2 million and KZT 630 million, about 300 individuals were involved.

Currently, the case has been completed and referred to court.

296. In addition to threshold and suspicious transactions, the FIU also receives information on transactions suspended by the obliged entities prior to their conduct, due to the presence of suspicion in ML/TF. Upon receipt of such information, the FMA examines it, decides within 24 hours to suspend the suspicious transaction for 3 business days and submits the information to LEAs/SSAs in accordance with their purview for taking a decision. LEAs/SSAs, which received the information, conduct appropriate police intelligence operations and, if there are indicators of a crime on the part of the suspended transaction participants, LEAs/SSAs have the right to extend the suspension period for another 15 days.

Table 6.8. Comparative statistics on suspended transactions and their use for 2017-2022.

	Number of transactions suspended by the obliged entities	**Number of transactions suspended by the FMA for 3 business days and forwarded to LEAs/SSSs**	**Number of transactions used by LEAs/SSAs that have been suspended by the FMA**
Suspended transactions	7 228	3 158	1 088

297. As noted in the table, 44% of the transactions suspended by the obliged entities following the FMA analysis were the basis for sending information to LEAs/SSAs for conducting appropriate PIA and 34% of the total number of transactions reported to the FMA were used by LEAs/SSAs to initiate criminal proceedings or gather evidence.

298. The FIU's authority allows it to request any additional information from the obliged entities (whether or not such entity has sent an STR) when analyzing available information for predicate and ML/TF offences, as well as trends and shemes of such offences. The FMA's interaction with the obliged entities to obtain additional information is conducted on an ongoing basis and in an automated format.

Table 6.9. Statistics of FMA requests for obtaining additional information from the obliged entities

Type of obliged entity	2017		2018		2019		2020		2021		1st half of. 2022	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
STBs	383	397	742	817	840	563	6797	768	45 909	842	11015	379
DNFBPs	0	0	4	1	2	1	5	1	4	0	15	0
FIs	11	3	18	28	18	45	77	105	1 219	151	61	82
Total:	**394**	**400**	**764**	**846**	**860**	**609**	**6879**	**874**	**47 132**	**993**	**11 091**	**461**

299. As this table shows, the FIU actively requests additional information from the obliged entities for conducting comprehensive tactical and strategic analysis. The increase in the growth of the FIU's requests for additional information since 2021 is justified by the project approach and operational and preventive measures of the FMA such as conducting large-scale operations named "Stop-Obnal" (identifying arrays of legal persons engaged in illegal cashing-out), "Kamkor" (identifying embezzlement of public funds allocated for the social sphere), "Kazyna" (identifying embezzlement of public funds), "Stop-Igra" (suppressing illegal betting and casino activities), etc.

Case Study 6.5. FMA Targetted approach

As part of the Stop-cash operation in 2019, suspicious transactions of Zh-K-A LLP were detected in Pavlodar, from whose account more than 99% of incoming funds were cashed out in the total amount of 373 million KZT.

The First Heartland Jusan Bank JSC received 71 reports of threshold and suspicious transactions in respect of Zh-K-A LLP, including 63 reports of cash withdrawals by citizen M. In order to evade financial monitoring, cash withdrawal amounts were divided into 46 transactions, each of which did not exceed 10 million KZT.

Banking operations on the company's accounts were suspended by the FIU, the relevant information was sent to the territorial department of EIS

07/19/2019 EIS started pre-trial proceedings on the fact of tax evasion by issuing counterparties without commodity invoices on behalf of 21 one-day firms controlled by an organized criminal group (hereinafter - OCG).

The investigation found that 11 members of the organized criminal group under the leadership of "M" used a complex scheme for cashing out funds by repeatedly transferring them between controlled enterprises. The total turnover of mutual settlements amounted to more than 8.4 billion KZT. The damage to the state in the form of unpaid tax payments amounted to 530 million KZT.

In order to legalize proceeds obtained by criminal means and conceal their true origin, expensive movable and immovable property was acquired with criminal funds in the names of close relatives of members of the organized criminal group “I”, “N”, “K”, “S”.

The total value of movable and immovable property amounted to 374 million KZT, which was also seized.

By the verdict of the court No. 2 of Pavlodar dated October 21, 2020. all 11 members of the organized crime group were found guilty under Article 262 (creation and participation in an organized crime group), 245 (tax evasion), 216 (extract without commodity invoices), 218 of the Criminal Code (money laundering) and sentenced to imprisonment for a term of 2 to 6 years, with confiscation of criminal proceeds in the amount of 20.3 million KZT, as well as movable and immovable property worth 374 million KZT.

3.2.3. Analysis and provision of materials by the financial intelligence unit for operational purposes

300. The FMA is the national center for gathering, processing and analysis of financial intelligence and

other information, as well as the competent authority for the prevention, detection, suppression, uncover and investigation of economic and financial offences within its purview.

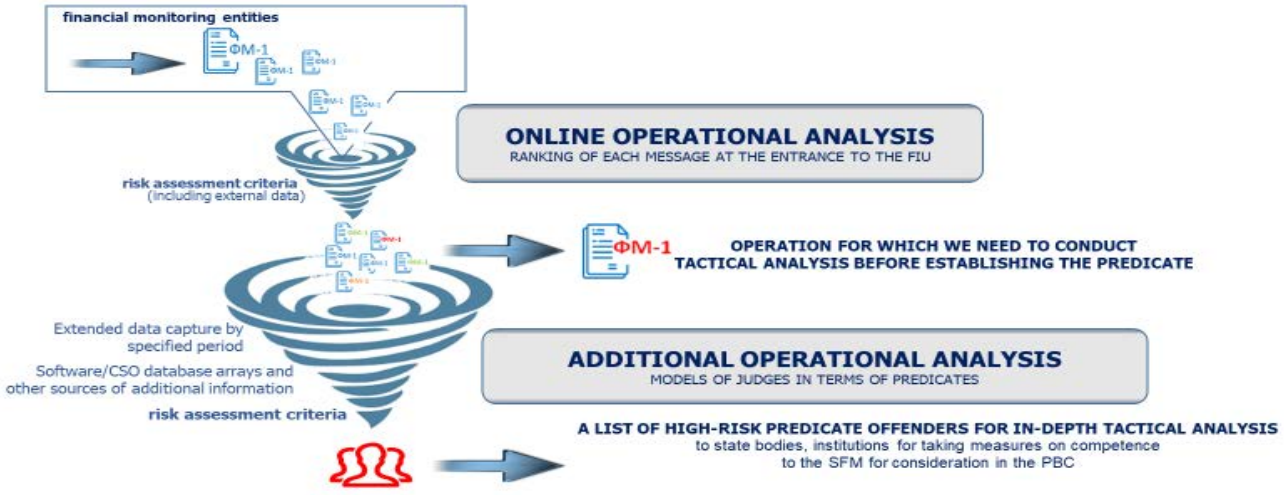
301. As described in Chapter 1, the FMA performs in analysis of STRs and other relevant information, the results of which are submitted to the EIS and LEAs/SSAs. The FIU has all the necessary tools and state-of-the-art IT resources to conduct quality operational, tactical and strategic analysis for combating ML/TF and predicate offences and providing quality materials to the EIS and LEAs/SSAs.

302. The FIU conducts financial investigations proactively on the basis of STRs/other information or at the request of LEAs/SSAs. Financial investigations are conducted by the FMA's specialized units, with a staff of 12 analysts for operational analysis, 73 for tactical analysis and 12 for strategic analysis. Due to the high degree of digitization of analytical work and automation of information processing, as well as the application of the risk-based approach to STR analysis, this number of analysts is sufficient for financial investigations.

303. All reports are submitted to the UIAS for operational (primary) analysis. At this stage, all reports are processed and ranked by previously approved indicators in order to identify riskier actors with respect to ML/TF predicate offences, which are subsequently forwarded for tactical analysis.

Operational Analysis

304. Operational analysis is performed by a separate dedicated FIU division. The analysis involves two stages: basic and supplementary.



305. At the first stage of operational analysis, the reports processed in the "Financial Transaction Data Collection" subsystem go to the "Operational Analysis" subsystem of the UAIS, which processes data as to involvement of the obliged entities in ML/TF. The subsystem determines the degree of risk of involvement of a financial transaction in ML/TF using the system's criteria for prioritizing and identifying high-risk transactions by level of suspicion. If transactions with a high ML/TF risk are detected, the UIAS generates and transmits a "high-risk" report to the appropriate analytical units of the FIU for tactical analysis.

306. As part of additional operational analysis of reports, all information received by the UIAS is ranked according to the predicate offences that have been assigned a high risk by the NRA. For this purpose, the FIU has developed 20 criteria that are refined based on the analysis of feedback from the FIU analytical units and LEAs/SSSs' work results, to whom proactive materials are forwarded. Additional operational analysis results in making is a list of high-risk persons broken down by predicate offence, which is submitted 1) to the FIU's analytical units for conducting in-depth tactical analysis; 2) to the RK SRC for registering in the internal risk management system and 3) published on the FMA website so that the obliged entities could consider it in their internal control rules.

307. The experts reviewed the prioritization and ranking criteria for STRs, which are approved by the FMA's internal orders (business requirements) and agree that these criteria are relevant and consistent with the identified ML/TF risks.

Tactical analysis

308. Tactical analysis is carried out by the FIU's specialized units formed according to the objects of analysis (ML, TF, PF, predicate offences). According to the Tactical Analysis Rules, when conducting tactical analysis, the analyst should:

- make a separate assumption for a particular predicate or ML/TF offence, which will determine further actions of the analyst;
- search and collect all transactions (threshold and suspicious) of the target of the analysis in the UIAS, obtain general information about the target from the Integrated Tax Information System;
- establish the kinship of the person involved in transactions and affiliated legal persons using the Information Exchange System of Law Enforcement and Special Authorities (relatives, search for information on participation in the activities of the legal person by holding a direct executive position or participating in the authorized capital, or the existence of close family ties with the person holding such positions, search for information on movable and immovable property of the persons involved, etc.);
- if necessary, make appropriate requests, including to the competent authorities of foreign countries;
- make a list of counterparties to suspicious transactions, in the activities of which financial transactions with high ML or TF risk have been previously identified;
- identify individual transactions with ML/predicate/TF/PF indicators;
- conclude whether there are elements of crime.

309. In order to improve the FIU's analytical activities, the aforementioned Tactical Analysis Rules are accompanied by risk indicators characterizing suspicious ML activity (29 indicators) and TF activity (14 indicators), which should be taken into account by the analyst when identifying suspicious activities of legal and natural persons. This list of risk indicators is not complete and is reconsidered/updated on a regular basis. According to the experts, it serves as an additional mechanism to reinforce the analysis conclusions.

310. In order to model, link the persons involved, work with big data and visualize analysis results, the FIU makes extensive use of analysis tools such as Qlik Sense, Oracle BI, IBM I2, Triton and SimBase in the course of its analytical activities. The use of such software products improves the analysis quality, ensures the timely transfer of materials to LEAs/SSSs and helps the user clearly reflect the elements of crime and identified offenders and draw conclusions on the further allocation of LEAs/SSSs' forces and resources.

311. Separate time frames are set for tactical analysis, i.e. for preparation of proactive materials not requiring in-depth analysis - 15 days, for materials requiring detailed study with the establishment of a multi-level scheme - not more than 30 days, and for preparation of responses to LEAs/SSSs' requests - not more than 30 days. If LEAs/SSSs request information that is already available to the FIU, such requests are processed more quickly. Representatives of LEAs/SSSs also confirmed that they received the requested information from the FIU in a timely manner.

312. The results of operational and tactical analysis generate financial intelligence that can only be used as intelligence (to identify suspects and conduct direct investigations), but cannot be introduced as evidence at trial. LEAs/SSSs use this data as a source for evidence and tracking criminal proceeds at the PIA stage and in criminal investigations.

Case Study 6.6. FIU submission of initiative material to the LEAs/SSAs

In 2017, the FIU revealed suspicious operations of LLP "B-G" in Pavlodar city and uncovered a criminal

scheme, according to which citizen Zh. was engaged in the acquisition, storage, transportation and sale of fuel and lubricants.

The turnover in the purchase and sale of fuel and lubricants amounted to more than 5.5 billion KZT.

On 04.07.2017, the initiative material of the FIU was transferred to the EIS, which initiated pre-trial investigation into the fact of transportation of fuel and lubricants without documents confirming their legal source of origin and tax evasion.

The investigation found that citizen Zh., carrying out criminal activities in the field of illegal trafficking of petroleum products, sold them on the basis of fictitious documents confirming the origin of fuel and lubricants. The total amount of sold petroleum products was more than 6.2 thousand tons for a total amount of 584 million KZT.

Damage in the form of tax evasion amounted to more than 879 million tenge.

The joint forces of the investigation and FIU found that criminal income was used to purchase assets to support illegal business, including gasoline tankers with trailers, a production base with an administrative building with an area of 212 square meters, a land plot and 5 tanks for storing fuel and lubricants, a railway dead end and storage facilities for fuels and lubricants with a total area of over 5000 square meters.

The total value of the arrested property obtained by criminal means amounted to 211 million tenge.

On 17.07.2018, Pavlodar city court found citizen Zh. guilty under Article 245 (tax evasion), Article 197 (purchase, storage, transportation and sale of fuel and lubricants without documents confirming the legality of their origin), Article 218 (legalization) of the CC and sentenced to 5 (five) years 6 (six) months imprisonment, with confiscation of criminal assets worth 211 million KZT.

313. Analysis of the materials sent by FIU both on a proactive basis, and upon request, and the effectiveness of the use of these materials by the LEAs/SSAs is presented in CI 6.1.

314. In general, the FIU uses modern technology and a high level of process automation to prioritize, initiate, and assist in LEAs/SSAs investigations.

Strategic analysis

315. The FIU conducts strategic analysis on an ongoing basis in order to identify ML/TF/PF threats, vulnerabilities and trends, to establish growth/reduction trends in types of transactions, cash flows and reports from the obliged entities. For this purpose, a separate FIU unit was established and an internal document approved the Strategic Analysis Rules, according to which such analysis is conducted at least once every six months.

316. During the strategic analysis, all received reports, FIU's own databases, information from the information systems of government authorities, the media, etc. are used. The findings of such analysis are prepared in the form of a report reflecting information by type of operation, region, obliged entities and other forms, and are sent to the relevant competent authorities and/or FIU's own divisions, taking into account the subject of the analysis conducted.

Table 6.10. Strategic analysis performed by the FIU

No.	Strategic analysis topics	Results are submitted to
1.	Detection of activities related to illegal outflow of capital	Supervisory authorities, obliged entities
2.	Investigation into international flows of funds as part of the "Orion" operations	CHFIU, FMA's analytical units
3.	Identification of specific indicators of unregistered business activities among natural persons in the banking sector	State Revenue Committee
4.	Analysis of cash flow between Kazakhstan and Russia	FIU of Russia, FMA's analytical units
5.	Analysis of cashing-out by legal persons in banks	FMA's Economic Investigation Service,

		General Prosecutor's Office
6.	Analysis of financial flows by indicators specific for pyramid schemes	FMA's Economic Investigation Service, General Prosecutor's Office
7.	Analysis of the public procurement and its relationship with shell companies for combating the embezzlement of public funds	Anti-Corruption Service, FMA's Economic Investigation Service
8.	Analysis of the "disruptive activity" funding	Presidential Executive Office, FMA's analytical units
9.	Analysis of foreign funding for non-profit organizations	Presidential Executive Office, FMA's analytical units

317. The typologies developed as a result of the strategic analysis are also sent to the obliged entities to improve their analytical component and the quality of their reporting.

Case Study 6.7. Use of Strategic Analysis

To develop effective measures to identify financial pyramids, the FMA, together with Kaspi Bank JSC, automated the business process in the “Financial pyramid” direction.

This tool allows you to automatically generate a scheme according to the bank statement of Kaspi Bank JSC. The scheme reflects summary information about depositors and recipients of funds, which will significantly reduce the time for analyzing the activities of alleged financial pyramids.

The system counts transactions, identifies systematic transactions, determines time periods, and so on. The scheme itself is formed taking into account the criteria reflected in the Typology related to the activities of financial pyramids

318. In general, conducting strategic analysis on an ongoing basis has a positive impact not only on the identification of ML/TF methods and techniques, crimes and criminal prosecution of predicate offenses, improving the quality of reports sent by the FIS, but also increases the effectiveness of the entire national system of Kazakhstan.

3.2.4. Cooperation and exchange of information/financial intelligence

319. Interaction and cooperation at the national level are the strengths of Kazakh AML/CFT system. The FMA, as a central element of the anti-money laundering system, has concluded 10 bilateral agreements with state regulators, law enforcement authorities and SRBs, as well as 30 such agreements with public associations, in order to organize effective cooperation for the exchange of AML/CFT information at the national level. At the international level, the FMA has entered into 39 memorandums of cooperation in the AML/CFT sphere with foreign FIUs and 10 agreements with competent authorities of foreign countries through the FMA's Economic Investigation Service.

Case Study 6.7. Example of interaction between the FIU and EIS

Due to the joint work of the FIU and EIS, a criminal scheme was revealed that was used by an organized criminal group in Nur-Sultan between 2015 and 2019 for the purpose of issuing fictitious invoices in order to assist in tax evasion in the amount of more than KZT 10 billion.

The obliged entities submitted 1,988 threshold and suspicious transactions reports amounting to KZT 41 billion in respect of a number of interrelated companies.

Banking operations on the company's accounts were suspended by the FIU and the relevant information was sent to the EIS. In addition to the suspended suspicious transaction, an assumption on suspicious activity of interrelated companies was made and sent.

On September 26, 2019, the EIS initiated pre-trial proceedings on tax evasion by issuing fictitious invoices to counterparties on behalf of 29 shell companies controlled by the organized criminal group under the direction of G.V.

Besides that, the main counterparty of the "cash-out" enterprises controlled by the organized criminal group was a construction company, the founder of which was a Turkish national "Esen", who, using

fictitious invoices, cashed out over KZT 2.0 billion in second-tier banks between 2015 and 2019, part of which he converted into foreign currency worth USD 2.1 million and withdrew to his account in Turkey.

The damage in the form of unpaid taxes amounted to KZT 850 million.

The investigation also found that in order to legalize the criminal proceeds of money laundering and tax evasion, they purchased expensive immovable and movable property worth more than KZT 250 million (4 luxury apartments and houses in Nur-Sultan, 4 luxury cars: 2007 Cadillac Escalade, 2002 Mercedes-Bens G500, 2012 Hyndai Tucson, 2010 Porsche Panamera).

On June 2, 2021, the court of the Saryarkinskiy District of Nur-Sultan found G.V. and 7 members of the organized criminal group guilty under Articles 262 *(establishment and participation in the organized criminal group)*, 245 *(tax evasion)*, 216 *(issuance of fictitious invoices)* and sentenced to imprisonment for a term of 6 to 8 years. Turkish national "Esen" was found guilty under Articles 245 *(tax evasion)*, 218 УК *(legalization of criminal proceeds)* and sentenced to imprisonment for a term of 7 years. Besides that, the court confiscated the criminal property worth more than KZT 250 million.

Case Study 6.8. On embezzlement of public funds and legalization of criminal proceeds

In 2018, the FIU identified suspicious transactions of individual E.H. in the Akmola Region. Information about this individual's suspicious activities was sent to the EIS for conducting an inspection.

The EIS in the course of the inspection uncovered a criminal scheme, according to which individual E.H. for personal profit embezzled public funds allocated to subsidize the development of livestock breeding, increasing the productivity and quality of livestock products, by deception and entering knowingly false information in an application for subsidies, as well as by submission of documents confirming the purchase of livestock in the Akmola Region.

The total economic damage caused to the state in the period from June to November 2017 amounted to KZT 20,498,230.

The EIS initiated pre-trial proceedings on the fact of embezzlement of public funds allocated in the framework of subsidizing the development of breeding livestock, increasing productivity and quality of livestock products.

The investigation found that E.H., carrying out criminal activities in the field of unjustified receipt of subsidies from the state budget, after receiving money from the Department of Agriculture of the Akmola Region to the account of IE "Yerlan" in the form of subsidies, on November 31, 2017, in order to legalize money obtained by criminal means, purchased a MTZ 80.1 tractor from S.A.K. LLP.

On August 23, 2018, the Zerendinskiy District Court found E.H. guilty under CC Articles 190 and 218 and sentenced to imprisonment for a term of 6 years and 6 months.

320. The positive aspect of Kazakh anti-money laundering system is that government authorities and LEAs/SSAs inform the FIU of suspicious transactions that have come to their attention in the exercise of their competencies. The experts believe that this informing is an additional impetus for the FMA in its analytical activities and strengthens interagency cooperation.

Table 6.11. Statistics of information received by the FIU from the government authorities and LEAs/SSAs.

	2017	2018	2019	2020	2021	1st half of 2022
Number of information received	126	241	227	216	292	176

321. AML/CFT information exchange between the FIU and LEAs/SSAs is carried out exclusively through the CERTEX secure communication channel, which corresponds to the third level of the state security standard of the Republic of Kazakhstan "ST RK 1073-2007 Means of Cryptographic Protection of Information" or through the courier service communications.

322. All LEAs/SSAs demonstrated awareness of the FIU's authority to promptly obtain relevant financial information from abroad and use this opportunity in practice. For 2017-2022, 30% of international requests sent by the FMA were initiated by the NSC and EIS, 64% of outgoing requests were sent by the FIU during the analysis of STRs and other information, and the MIA and ACA initiative to obtain information through international cooperation of the FIU was 3% each (see IO.2). Information received via international channels is transmitted to LEAs/SSAs subject to the consent of the FIU that provided such information. All transmitted information is marked as restricted (for official use or confidential) and protected in accordance with the law.

323. The quality of submitted FMA materials and the results of the use of this information by LEAs/SSAs are assessed by receiving feedback in the form of reconciliation acts involving the FMA, LEAs/SSAs and GPO. The completed reconciliation acts are communicated to the relevant FMA performers for identifying the areas of further analytical activities.

324. The UIAS users are audited on an ongoing basis by officers of the FMA's Information Security Directorate for lawful use only within the scope of official duties. The FMA's local network is divided into internal and external, and these networks are protected by CISCO firewalls. The UIAS is located in the internal network, which is not accessible from the outside. All information is withdrawn by analysts from the internal network only through a dedicated room, which is controlled and monitored by the Information Security Directorate.

325. The FMA building is a secure facility, which is guarded by the RK MIA's Police Regiment for Government Authorities Protection.

Overall conclusion on Immediate Outcome 6

326. A wide range of financial and other information is available to all LEAs/SSAs. LEAs/SSAs regularly and effectively request, receive (including proactively) and use the FIU financial investigation data and other relevant information to gather evidence for investigating money laundering, terrorist financing and predicate offences and tracing criminal proceeds. The FIU is a core element of the national AML/CFT regime in Kazakhstan and has a vast amount of data at its disposal. The FIU uses modern technology and a high level of process automation to prioritize, initiate and assist in investigations of cases conducted by LEAs/SSAs. Most threshold and suspicious transaction reports are received by the FIU from FIs. The FIU also receives other additional information from STBs upon request. The FIU also receives information on transactions suspended by the obliged entities before they take place due to the suspicion of ML/TF. The protection of information and intelligence exchanged by the competent authorities is ensured.

327. LEAs/SSAs, namely the FMA's own operational and investigative units actively request information from the FIU on high-risk predicate offenses (except illegal economic activity and drug trafficking) and ML, while information on combating TF is less actively requested by relevant competent authorities, while the referral by the FIU of proactive materials on TF tends to decrease. The MIA and the ACA made less use of the FIU's ability to obtain relevant financial information as part of international cooperation.

328. **The Republic of Kazakhstan is rated as having a substantial level of effectiveness for IO.6.**

3.3. Immediate Outcome 7 (ML Investigation and Prosecution)

3.3.1. ML identification and investigation

329. Detection, suppression and solving of ML offences in the Republic of Kazakhstan are carried out in the form of criminal intelligence and detective activities (CIDA) and pre-trial investigations (more - R.30).

330. The basis for the exercise of powers by a body engaged in the CIDA is any information about ML or predicate offence. When information about an offence is confirmed in the course of the CIDA, this information is registered in the URPI and transferred in accordance with the investigative jurisdiction for pre-trial investigation.

331. An FIU's proactive information on the suspicious transaction report is also grounds for initiating a pre-trial ML investigation.

Case Study 7.1 Use of the FIU proactive reports

The FMA forwarded the information to the investigative unit of the EID in the Pavlodar Region about a suspended suspicious transaction involving Kazakh national N., who intended to make an international transfer of funds in the amount of USD 700 thousand from his bank current account in the RK to a bank current account opened in his name in a foreign country. As a result of the FIU's analysis, it was found that the transaction was of a dubious nature and possibly related to illegal capital outflow.

Materials received from the FIU were registered in the URPI, and a pre-trial investigation was initiated against N. under CC Article 218(3) - legalization of criminal proceeds in a large amount and the indicia of the predicate offence had not been established at the time the ML case was initiated.

332. In cases of ML offences, the pre-trial investigation is carried out in the form of a preliminary investigation, in which the investigator, in accordance with the provisions of the criminal procedure law, proves the fact of ML, establishes its elements and exposes the guilty persons.

333. ML can also be identified as part of a pre-trial investigation into a predicate offence through investigative actions or police intelligence operations conducted by a body engaged in the CIDA by the investigator's instructions. In this situation, the ML offence is registered and combined in one proceeding with the predicate offence criminal case.

Case Study 7.2 Identification of ML during the pre-trial investigation of a predicate offence

During the pre-trial investigation into the criminal case against K. under CC Article 189(4), Par. 2, it was established that the offender, having committed a large-scale theft of public funds in order to conceal the source of the criminally obtained funds and introduce it into the legal circulation, deposited KZT 6.5 million on his personal account in a betting company. Later, under the guise of getting the bet winnings, he cashed out the specified funds, disposing of them at his own discretion. A pre-trial investigation under CC Article 218 was additionally initiated against K., the cases were combined in one proceeding.

According to the sentence of June 25, 2019, K. was found guilty of theft in an especially large amount and legalization and sentenced to imprisonment for a term of 7 years for the totality of the crimes committed.

334. Since the law establishes an alternative jurisdiction for ML crimes, the criminal case is usually investigated by the body that identified ML. The only exceptions are cases of revealing a fact of ML committed by a special category of criminals - a person authorized to perform state powers or holding an important public position (the case is referred for pre-trial investigation to the ACA), as well as cases where the prosecutor takes over the investigation or refers the case for investigation to another authority.

335. The legality of the CIDA and pre-trial proceedings is supervised by prosecutors by authorizing the particularly police intelligence operations, coordinating investigative actions and issuing written instructions binding on investigators.

336. At the pre-trial investigation stage, investigative actions (seizure of property, inspection, search, removal, applying a restrictive measure, designation in the international wanted list, etc.) are authorized by a court.

337. If the fact of ML is not proved, the pre-trial investigation into the criminal case is terminated. Termination of the case does not entail a negative assessment of the fact of initiating the CIDA and pre-trial ML proceedings.

338. At the end of the pre-trial investigation, the criminal case is sent to the prosecutor for referral to court. The prosecutor may return the case to the pre-trial investigative authority for additional investigation or

send it to court for consideration on the merits.

339. Prosecutors represent the state prosecution in a court hearing. Based on the results of the trial, the court makes the final procedural decision on the case. If the prosecutor disagrees with the verdict, he has the right to appeal it to a higher court.

340. Thus, there are no obstacles in the Republic of Kazakhstan to the exercise by LEAs/SSAs of their powers to detect ML and prosecute these offences. The basis for the exercise of these powers is any information, including information on the suspicion of ML. At the same time, the competent authorities are not bound by the framework of the proceedings in the case of a predicate offence and do not consider ML detection as a secondary task. The alternative investigative competence established by law in criminal cases of ML offences is also a positive factor that mobilizes all competent authorities to detect these crimes.

341. Analysis of the criminogenic situation in the Republic of Kazakhstan shows a significant reduction in criminal offences. The total number of crimes registered in the URPI in 2021 compared to 2017 decreased by 50% (see also Chapter 1 and IO.1).

342. There were also adjustments in the criminal law. The amount of damage from economic offences, which entails criminal prosecution, has been significantly increased. Full reimbursement of damage, payment of income obtained by criminal means are established as grounds for exemption from criminal liability for certain acts (illegal entrepreneurial activity, creation and management of pyramid or Ponzi schemes, tax evasion, etc.). The amendments to the criminal law to some extent have led to a reduction in the number of ML investigations for these predicate offences since in order to be exempt from criminal liability the perpetrator returns to the state the entire proceeds of crime, which eliminates the possibility of involving such proceeds in laundering.

343. According to the country's information, such adjustments made it possible to bring delicts that do not have the public danger inherent in criminal acts into the sphere of administrative legal proceedings and exclude criminal prosecution for acts that do not go beyond civil law relations. Generally agreeing with this assessment, the experts note that such changes in the legal regulation are positive, since they are aimed, *inter alia*, at increasing the efficiency of the pre-trial investigative authorities.

344. Thus, the priority in the country is criminal prosecution for serious offences that accumulate criminal proceeds in a significant amount, thereby creating high ML risks. If the threshold of criminal liability is not reached (for those offences where it is established), other mechanisms within the framework of tax and customs administration (additional charges and collection of tax and customs payments), administrative and civil proceedings (bringing to administrative responsibility, invalidation of civil-law transactions, etc.) are applied, allowing to ensure the removal of unjustified income and compensation for the damage caused.

345. According to the information provided, a total of 298 ML offences were registered in 2017-2021, including: in 2017 - 81, 2018 - 79, 2019 - 42, 2020 - 40, 2021 - 56. The decrease in the detection of ML cases from 2017 to 2020 correlates with the crime situation in the country.

346. The breakdown of the number of ML cases (CC Article 218) reported in 2017-2021 by agencies is shown in the table below.

Table 7.1. Number of registered ML cases.

	2017	**2018**	**2019**	**2020**	**2021**	**Total**
EIS	46	41	30	24	33	174
ACA	15	29	5	5	1	55
NSC	8	2	4	4	18	36
MIA	11	7	3	7	4	32
GPO	1	-	-	-	-	1
Total	**81**	**79**	**42**	**40**	**56**	**298**

347. The data shows that the main burden of detecting and prosecuting ML offences is carried out by the EIS (58.4% of the total number of recorded ML offences).

Table 7.2. Breakdown of the number of ML criminal cases registered by the EIS by predicate offence

Predicate offence:	2017	2018	2019	2020	2021	Total
Misappropriation or embezzlement of entrusted third party's property (CC Article 189)	-	6	5	7	7	25
Fraud (CC Article 190)	10	7	1	-	5	23
Infliction of pecuniary loss by deception (CC Article 195)	-	1	-	-	-	1
Illicit trade in crude oil and petroleum products (CC Article 197)	6	8	5	2	3	24
Economic offences						
Illegal entrepreneurship, banking activities (CC Article 214)	5	-	-	-	-	5
Issuance of fictitious invoices (CC Article 216)	4	7	7	9	9	36
Setting up a pyramid scheme (CC Article 217)	-	-	-	-	4	4
Production, storage or sale of counterfeit money (CC Article 231)	-	-	-	1	-	1
Breach of excisable goods marking procedure (CC Article 233)	-	1	-	-	-	1
Economic smuggling (CC Article 234)		1	-	-	2	3
Tax evasion (CC Article 245)	5	8	3	-	2	18
Other offences						
Illegal gambling operation (CC Article 307)	13	2	8	5	1	29
Document forgery (CC Article 385)	-	-	1	-	-	1
ML cases without simultaneous investigation into predicate offences	2	-	1	-	-	3
Total	45	41	31	24	33	174

348. Of the total number of offences detected and investigated by the EIS, 25 (14.4%) were committed by organized criminal groups.[14] There are case studies of successful detection and prosecution of this type of criminal activity, which due to its organized form poses a high danger to the state and society.

Case Study 7.3. Laundering of criminal funds by an organized criminal group identified by the EIS

An organized criminal group under the direction of T. was engaged in illegal entrepreneurial activity - artisanal production of alcoholic beverages and their sale with counterfeit accounting and control stamps. The proceeds from the sale of these products amounted to KZT 271 million (more than USD 830 thousand). In cooperation with the FIU it was established that part of the criminally obtained funds was legalized by the members of the OCG through the purchase of movable and immovable property (vehicles, residential building), fictitiously registered as the property of close relatives of the offenders. The said property, the value of which amounted to KZT 20 million (USD 61 thousand), was seized during pre-trial proceedings. The organized group members were sentenced by the court for the totality of the crimes covered by CC Articles 262 (participation in an organized group), 233 (violation of the procedure and rules of labelling excisable goods), 214 (illegal entrepreneurial activity) and 218 (ML) to imprisonment for a term of 5 to 7 years. The legalized property was confiscated into state revenue.[15]

349. According to information provided by the ACA, the predicate offences for ML detected by the agency were theft by misappropriation or embezzlement (CC Article 189) - 22 (40% of the total number of ML cases reported in 2017-2021), bribe-taking (CC Article 366) - 13 (23.6%), abuse of power (CC Article 361) - 11 (20%), fraud (CC Article 190) - 6 (10.9%). One ML case was detected in criminal cases of illegal gambling operation (CC Article 307), organizing a brothel for the purpose of prostitution (CC Article 309), and excess of power or official powers (CC Article 362).

350. A significant decrease in the number of detected ML offences was explained by the decrease in the total number of pre-trial criminal cases investigated by the ACA (43% less in 2021 than in 2017). In addition, they pointed out that a significant number of corruption offences are detected in the framework of

[14] According to the RK legislation, establishment, direction and participation in an organized group, criminal organization, criminal community, including transnational ones, constitute independent offences. Actions of the participant of the criminal group receive legal assessment for the totality of the crimes committed - directly for participation in such group and for the concrete offences committed as a part of it.

[15] Hereinafter the amounts in USD are given according to the official average annual exchange rate for USD 1: KZT 326 in 2017, KZT 344,71 in 2018, KZT 328,75 in 2019, KZT 412,95 in 2020, KZT 426,03 in 2021 (www.online.zakon.kz)

CIDOs, persons are apprehended immediately upon committing a crime (e.g. while taking a bribe), thus they have no opportunity to dispose of the criminal proceeds and involve them in the ML.

Case Study 7.4. Suppression of a corruption offence at the stage of obtaining criminal proceeds

In order to receive a bribe, the head of a subdivision of the district executive authority (akimat), V., arranged for the signing of a fictitious certificate of accomplishment, on the basis of which budget funds in the amount of KZT 3.5 million (approximately USD 8.2 thousand) were transferred to the bank account of D.'s enterprise. Having withdrawn the money from the company's bank account, D. gave V. as a bribe KZT 2 million (about USD 4,700) as a bribe. V. was detained red-handed by ACA officers and the subject of the bribe was seized.

V. for taking bribes and D. for giving bribes were sentenced to three years imprisonment with life imprisonment and deprivation of the right to hold public office. The subject of the bribe (KZT 2 million) was confiscated for the benefit of the State.

351. At the same time, taking into account that facts of a long period of committing corruption crimes due to their latent nature, generation of criminal income in a significant amount are not excluded, the reasons mentioned by the agency do not fully explain the downward trend in the detection of ML from corruption crimes.

Case Study 7.5. Detection by the ACA of laundering of funds obtained through a corruption crime

B., as an official, head of the Shymkent Department of Architecture and Urban Planning, when conducting a public procurement of works for carrying out a topographical survey of urban communications, in order to steal public funds, ensured that A., director of a private company, which had no license to carry out such a survey, won the tender. On the basis of fictitious documents on the allegedly completed work, public funds in the amount of KZT 498 million (USD 1.3 million) were transferred to the company's bank account, of which A. cashed out KZT 354.8 million (USD 927 thousand). In order to legalize the money, B. purchased a land plot where he built a business facility with their fictitious registration in the ownership of third parties. The legalized property value amounted to KZT 130.6 million (USD 341.3 thousand). The court found B. and A. guilty of embezzlement and B. also of legalization (ML) and sentenced B. to imprisonment for a term of 10 years and A. - for a term of 8 years with life-time deprivation of the right to hold certain positions. The legalized property was confiscated. The state recovered from the offenders a total amount of KZT 498 million as compensation for material damage.

352. The MIA is the central LEA engaged in combating illicit trafficking in narcotic drugs, psychotropic substances, their precursors and analogues. According to the information provided by the agency, the level of illicit drug trafficking in the country is high. The country's understanding of the importance of suppressing the financial basis of drug crime and introducing the funds derived from the sale of psychoactive substances into legal circulation is high. In 2017-2021, the MIA uncovered 21 cases of laundering drug proceeds, accounting for 65,6 percent of all ML cases detected and suppressed by the agency.

Case Study 7.6. Detection of the ML of drug proceeds by the MIA

A. organized and directed a criminal group, which sold heroin on a particularly large scale in the territory of the Republic of Kazakhstan. The payment for the drugs was made by consumers through the transfer of funds to the accounts of "QIWI-wallets" of the Russian bank. In cooperation with the FIU, it was found that in order to legalize and introduce them into legal circulation, the criminally obtained funds were transferred to bank accounts in Kazakhstan, registered to close relatives of A., cashed by him and used at his discretion. The amount of legalized proceeds was more than KZT 9 million (more than USD 20 thousand). A. was sentenced for the totality of the crimes committed to imprisonment for a term of 18

years and confiscation of property for establishing an organized group, illicit drug trafficking and money laundering.

353. Despite the decrease in drug trafficking, the level of crime remains high and the amount of criminal income generated is significant. At the same time, the number of detected instances of ML in relation to the total number of cases of drug sales is not significant. In this regard, it appears that efforts to detect money laundering from this category of predicate offences need to be stepped up.

354. In other criminal cases of ML offences detected by the MIA, the predicate offences were fraud, theft, theft by misappropriation or embezzlement, extortion, illegal migration and human trafficking.

355. In carrying out activities to detect and prosecute offences that trespass against national security, the NSC has identified the facts of laundering money derived from theft, corruption crimes, illicit drug trafficking and other offences (examples of the detection of cases by the NSC are given later in the text).

356. Statistics on the forms (methods) of laundering the proceeds of crime are collected analytically. by the country. The predominant form of ML is self-laundering (purchase of movable and immovable property by individuals for criminally obtained funds with its fictitious registration in the ownership of third parties, involvement in the economic turnover of legal entities under the guise of legally acquired production equipment, real estate), which corresponds to the risk profile of the country. There have been facts of the detection of ML by third parties.

357. The issue of prosecution of independent ML in relation to the legal system of Kazakhstan has a certain specific context. The legislation does not require mandatory investigation of the predicate offence together with ML, such acts can be combined in one proceeding or investigated independently. A characteristic feature of Kazakhstan's legal system is the principle of inevitability of criminal liability. In practice, this means that when ML is detected, the competent authorities take all measures to collect evidence that the laundered property has been obtained by criminal means. When a predicate offence is identified in a ML investigation, the cases are merged and the person is subsequently convicted of both the predicate offence and the ML offence. According to the information provided, in 2021-2022 14 ML cases were initiated (MIA - 8, FMSA - 6) without investigation for the predicate offence, subsequently predicate offences were identified within the ML investigation, and the cases were combined into one proceeding. While there have been no cases where stand-alone ML has been sent to court, based on legislation and communication with prosecutors and the judiciary, experts have ascertained that where the prosecution of a defendant for a predicate offence is terminated, a conviction for ML is still not excluded, unless the termination of prosecution for the predicate offence was linked to the absence of the predicate offence as such (i.e. the action was not a crime), respectively the proceeds derived from person's actions are, not criminal too.

358. Thus, it is possible to prosecute for a stand-alone ML in the Republic of Kazakhstan.

Mechanisms and resources used by competent authorities to detect ML.

359. Information on the staffing level of LEAs/SSAs is confidential, it can not be included in the report. However, the information on staffing numbers was provided to the experts by the competent authorities, by virtue of which experts concluded that the available staffing capacity was sufficient for performing all the tasks assigned to the agencies.

360. Each LEA/SSA has specialized operational units engaged in conducting the CIDA and investigative units (offices, departments) engaged in pre-trial proceedings. Interaction between operational officers and investigators and control over their activities are regulated by legislative acts (Law 154-XIII, CPC) and departmental local acts.

361. To ensure the prioritization of investigations into criminal cases of predicate offences with a high degree of ML threat and ML offences, the investigation is entrusted by the heads of investigative units to investigators based on their experience and qualifications. For the investigation into particularly complex

cases, operational investigative groups are created. If necessary, investigations may be carried out by a group of investigators, as well as referred from the territorial division to the central offices of agencies.

362. Investigative action plans are drawn up for criminal cases and their implementation is monitored by heads of investigative units. They are also empowered to analyze criminal cases and give instructions to investigators concerning them. Case studies of investigative action plans and instructions from the heads of investigative units are provided to the experts, including the instructions given in predicate offence cases for the purpose of identifying ML elements.

363. There are specialized prosecutors in the prosecutor's offices who conduct pre-trial investigations. Since prosecutors take on cases in exceptional cases (significant publicity or cases of particularly grave crimes), no ML cases were investigated by prosecutors in the assessed period. The role of prosecutors at the pretrial stage in ML cases was to supervise the procedural decisions taken by the criminal prosecuting authorities and to give binding instructions.

Case Study 7.7. Prosecutor's supervision of a criminal case on ML

A criminal case against K. for money laundering was terminated by a decision of a preliminary investigation authority for lack of corpus delicti. Having checked the legality of this procedural decision, the prosecutor refused to approve the resolution to terminate the criminal case. He gave written instructions to conduct investigative actions (interrogation of witnesses, holding confrontations, obtaining documents and others). The criminal case was sent for additional investigation.

364. The experts positively assessed the establishment of special units within the EIS and ACA, which are solely responsible for conducting parallel financial investigations. The officers of these units are included in the departmental operational investigative groups and conduct investigative actions in order to identify ML facts, determine the amount of criminal income received, search and seize property to secure its confiscation, and other investigative actions related to the investigation of the financial component of the crime.

365. The absence of special units in the MIA and NSC is not a significant disadvantage, since parallel financial investigations are conducted by these agencies, examples of successful investigations are given in the text. However, the experts believe that the establishment of such specialized units in the MIA and the NSC will further improve the effectiveness of financial investigations in these LEAs.

366. In the Republic of Kazakhstan consistently implements the "follow the money" principle. Parallel financial investigations are conducted by the competent authorities for establishing the facts of criminal obtaining of property, its location, schemes of ML of proceeds of crime, possession and use of the property for TF. Before the introduction in 2022 of unified methodological guidelines for their conduction, mandatory for all agencies engaged in combating ML/TF, the investigation of the financial component of criminal activity was governed by the instructions of the General Prosecutor and intradepartmental regulations. The purpose of creating a unified document was to consolidate the established practices of all competent authorities.

367. There are no separate statistics on parallel financial investigations in the country since they are conducted for all ML and predicate offences (both in the course of the CIDA and in pre-trial proceedings). This is due to the provisions of the criminal procedure law, according to which the fact that the property was obtained illegally or is the income derived from illegally obtained property, an instrument of crime or intended to finance terrorist activities or criminal groups shall be proved.

368. There are case studies of successful parallel financial investigations that allowed to uncover of ML offences and identify a significant amount of criminal property.

Case Study 7.8 Parallel financial investigation

The FIU detected suspicious transactions of company "A", from whose account 99% of incoming funds were cashed out. The bank transactions were suspended by the FIU and the information was submitted

to the EIS. During the pre-trial investigation, they found that an organized criminal group that consisted of 7 individuals and was directed by B., using 16 shell companies, avoided paying taxes by issuing fictitious invoices and caused damage to the state in the amount of KZT 36 billion (over USD 110 million). The criminally obtained funds were cashed out using a complex scheme of transfers between the controlled enterprises. During the parallel financial investigation it was established that with the purpose of laundering of criminal property and concealment of its true origin, an organized criminal group acquired 43 units of cargo vehicles, 123 units of immovable property (land, residential and commercial premises) fictitiously registered as the property of housekeeper B. The above property worth KZT 2,1 billion (over USD 6,4 million) was seized.

The court convicted the organized group members under CC Article 262(1,2) (establishment and participation in an organized criminal group), CC Article 245(3) (large-scale tax evasion), CC Article 216(3) (issuance of fictitious invoices), CC Article 218(2) (ML) to imprisonment for a term of 6 to 10 years with confiscation of legalized property.

Case Study 7.9 Parallel financial investigation

A criminal case on fraud and ML is under investigation by the EIS against D., who, in a group with other individuals, stole money in the amount of KZT 1.1 billion (over USD 2.7 million) through an illegal refund of corporate income tax. As part of a parallel financial investigation, it was found that D. in order to legalize criminal income in Astana acquired 23 land plots, fictitiously registered as the property of third parties, which he later sold to a construction company for 249 apartments in residential complexes under construction. These real estate objects registered as the property of a close relative of D. were sold. The laundering proceeds amounted to KZT 3.5 billion (approx. USD 8.5 million). The property of the suspects was seized in the amount of KZT 2.3 billion (more than USD 5.5 million).

369. Other case studies of successful parallel financial investigations are provided in IO.8.

370. The findings of parallel financial investigations are constantly analyzed by the agencies in order to develop measures to improve their tactics and methodology. The EIS has introduced an investigator ranking system, which is formed from indicators of the total number of cases under investigation, cases completed, and others. The highest ratings are assigned for detecting and investigating ML offences, successfully conducting parallel financial investigations, identifying criminal assets abroad and seizing such assets. Based on the ratings, the agency's senior management makes decisions on financial incentives for employees, career promotions and other rewards.

371. LEAs/SSAs have access to a wide range of information on natural and legal persons, including financial intelligence, for the purpose of conducting parallel financial investigations and exercising other powers (see IO.6). In this regard, the competent authorities have online access to the registration data of legal and natural persons, data on movable and immovable property, notarial and enforcement actions, state border crossings, customs declarations, tax returns, electronic invoices, purchase of rail and air transport tickets, criminal and administrative liability records, etc.

372. Besides that, agencies are developing internal information and analytical systems that allow them to accumulate and process large amounts of information, conduct tactical and strategic analysis and find links between natural and legal persons for the purpose of identifying ML and predicate offences.

373. Promptness of criminal prosecution is facilitated by the introduced form of conducting pre-trial inquiries in electronic format through the "Electronic Criminal Case" module by filling out data and requisites of electronic forms in the URPI, creating electronic documents and their signing using electronic digital signature or special signature tablet. Authorization of investigative actions is also carried out in the electronic format.

374. In addition to financial investigation units LEAs/SSAs also established specialized analytical units that provide information and analytical support for the activities of operational and investigative units,

including analytical identification of criminal schemes for predicate offences, development of ML typologies, preventive measures, proposals to improve the effectiveness of interagency cooperation and legislation.

375. All the competent authorities highly appreciated the cooperation with the FIU. Its legal framework is regulated by a number of bilateral and multilateral agreements, memorandums, roadmaps and plans. There are a significant number of case studies of detecting predicate and ML offences based on the FIU proactive materials, as well as the usefulness of the FIU information received in response to requests by LEAs/SSAs. Specific case studies are given above, as well as in IO.6.

376. LEAs/SSAs interact with the FIU by exchanging information on new schemes and methods of predicate and ML offences, identifying ML/TF vulnerabilities and participating in the joint development of measures aimed at mitigating the risks of predicate and ML offences.

Case Study 7.10. Information exchange

In 2020, the EIS uncovered a case of embezzlement by a social pedagogue of child-care institution residents' money coming to them as survivor and disability benefits. Having a power of attorney on behalf of the child-care institution to open current accounts with STBs and perform other banking transactions, the pedagogue gained access to the accounts and PIN codes of the residents. The children's funds were transferred to his personal accounts via bank applications and subsequently cashed out. The EIS and FIU developed a typology of this predicate offence. Besides that, a list of child-care institution residents (more than 2,500 children) was made, which the FIU disseminated to STBs with instructions to recognize the transaction (attempt) to withdraw (transfer) money from children's accounts as suspicious and inform the FIU of such transaction in accordance with the AML/CFT legislation.

377. The level of interagency cooperation between LEAs/SSAs is high. In the context of criminal prosecutions, the practice of conducting joint CIDO is widespread, as well as the investigation into the most complex multi-episode cases as part of interagency operational investigative groups for investigating predicate crimes and ML.

378. According to the ACA, between 2017 and 7 months of 2022, the agency officers were part of 61 interagency operational investigative groups established by the GPO, EIS, NSC and MIA. The ACA initiated the establishment of 14 such groups. The EIS initiated the establishment of 40 interagency operational investigative groups.

379. If necessary, officers of other government authorities and organizations (for example, tax and customs authorities of the SRC, officers of expert units, etc.) are involved in the investigation as specialists, who are assigned to conduct audits, inspections, examinations and analyses relating to their activity area.

380. Case studies of the detection and investigation of cases of serious and especially serious crimes by interagency operational investigative groups were submitted by the competent authorities.

Case Study 7.11 Investigation by operational investigative groups

Investigation into a criminal case against the chairman of one of the Kazakhs banks and other individuals for misappropriation of bank funds and abuse of power by issuing illegal loans against the interests of a financial institution was completed by the ACA and MIA interagency operational investigative group.

During the investigation into the criminal case, the schemes of illegal issuance of 66 loans to controlled persons in the total amount of KZT 22.5 billion (over USD 52.8 million) were established. The sum of voluntary compensation for damage amounted to KZT 9.2 billion (USD 21.6 million). The property was seized in the total amount of KZT 5.4 billion (USD 12.7 million). The case is currently under consideration in court.

381. LEAs/SSAs actively use mutual legal assistance mechanisms and other forms of international cooperation to fulfil their criminal prosecution tasks. Case studies were given of the successful detection of

the transfer of assets abroad, including ML committed abroad, as well as the seizure of criminal property located abroad.

Case Study 7.12. ML committed abroad

The NSC during the investigation into a criminal case against Kazakh nationals on charges of large-scale embezzlement of public funds in the course of state procurement under the state defence order established that D. legalized part of his criminal income by purchasing movable and immovable property (two cars, an apartment, a residential house and non-residential premises) with fictitious registration in the ownership of third parties. D. converted part of the criminal income to US dollars in the amount of 220 thousand, which he took out of Kazakhstan in cash. In order to legalize the criminal income in a foreign country, D. purchased a three-room apartment in the capital of one of the CIS countries with the criminally obtained funds, fictitiously registering it as the property of his common-law wife.

These facts were revealed as part of a parallel financial investigation in cooperation with the FMA and GPO, as well as using the tools of international cooperation, namely requests through EGMONT and CARIN network, and sending a request for mutual legal assistance in the form of the seizure of property, which was considered and granted by the competent authority of a foreign country.

The court found D. guilty of organizing grand theft and large-scale money laundering and sentenced him to imprisonment for a term of 11 years for the totality of the crimes committed. Proceeds of crime and criminal property, including an apartment in a foreign country, were confiscated into the revenue of the Republic of Kazakhstan.

Currently, a sentence for the confiscation of the said real estate in a foreign jurisdiction is being enforced as part of mutual legal assistance.

382. In addition to sending and executing requests for mutual legal assistance, such form of implementation of their powers as participating in foreign jurisdictions in the execution by foreign competent authorities of investigative and other procedural actions (Switzerland, Russia, UK, Belgium, UAE, Ukraine, Hungary, Uzbekistan, etc.) is used.

Case Study 7.13 Cooperation with foreign partners

The Ministry of Justice of the Kingdom of the Netherlands granted the request of the Kazakh GPO to participate in the investigation into the criminal case against A. suspected of embezzlement of public funds in the amount of more than USD 2,9 million and designated in the international wanted list by Kazakhstan. The ACA and GPO officers participated in searches, seizures and interrogations of witnesses conducted by representatives of the Dutch Financial and Corruption Investigation Office, during which they obtained evidence of A.'s criminal activities. The pre-trial investigation into the case is currently underway.

383. The training programs of departmental educational institutions, quantitative data on the LEAs/SSAs, prosecution and judiciary staff members who attended special training courses on ML detection and prosecution, information on the number of workshops, pieces of training and other training and methodological activities submitted during the on-site mission show that the country pays considerable attention to ensuring the availability of highly qualified staff in LEAs/SSAs and courts.

384. For improving the efficiency of prosecution authorities, educational institutions, in cooperation with the GPO and FMA, develop methodological materials, recommendations and guidelines. The experts were provided with such materials on conducting parallel financial investigations, search and return of criminal assets moved to foreign jurisdictions, mutual legal assistance.

385. Thus, the powers of pre-trial investigative authorities to identify, suppress and investigate ML offences are implemented in accordance with the legislation of the Republic of Kazakhstan and taking into account the specific anti-crime tasks performed by each agency within its purview. In general, this work is

carried out in a systematic manner.

386. The competent authorities have demonstrated the availabilities of necessary human, information and analytical resources. The country consistently implements the "follow the money" principle, has taken measures to improve the methodology of parallel financial investigations and has provided access to a wide range of necessary financial information. The level of interagency cooperation is high. International cooperation is used for the purposes of combating crime in general and ML in particular. All of these factors ensure the successful detection and prosecution of ML resulting from various predicate crimes, including those involving large-scale laundering of criminal proceeds committed by organized groups.

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

387. The ML NRA was conducted with the participation of pre-trial investigative authorities. The NRA's conclusions were based, inter alia, on criminal statistics provided by LEAs/SSAs, materials of financial investigations and criminal cases and judicial practice. The threat of ML was understood as unlawful actions of persons associated with the infliction of property damage and generation of income. The criteria for classifying predicate offences as acts with a high degree of ML threat were their share in the total number of crimes, the amount of damage and criminal income and the frequency of crimes committed by organized groups.

388. According to the NRA, high ML threats include tax crimes (fictitious invoices, tax and customs duties evasion, economic smuggling), illegal economic activities (illegal business activities, shadow turnover of oil and petroleum products, illegal gambling), corruption and embezzlement of public funds, fraud (including pyramid schemes), illicit drug trafficking.

389. The NRA findings are taken into account in program and strategic documents defining the national AML/CFT policy, such as the Comprehensive Action Plan for Suppressing Shadow Economy for 2021-2023 (adopted by RK Government Resolution No. 644 dated September 21, 2021), ML/TF Risk Mitigation Measures (adopted by RK Government Resolution No. 915 dated December 20, 2021) and others, as well as in documents of departmental and interagency nature that define strategic and tactical objectives of pre-trial investigative authorities and areas of their interaction with each other, as well as with other government authorities and organizations.

390. During the on-site mission, prosecutors demonstrated a good understanding of ML threats and risks. Importantly, their efforts focused not only on identifying and disrupting high-risk predicate offences but also on applying preventive measures that help reduce vulnerabilities and mitigate risks.

391. Countering predicate offences with high ML threat is carried out by pre-trial investigative authorities on a systematic and comprehensive basis by taking operational and preventive measures in the form of special operations. Their procedure, goals and objectives are defined by interagency plans, orders and roadmaps.

392. In order to suppress the activities of shell companies, reduce the number of fictitious invoices, and the level of criminal encashment, a special operation named "Stop-Obnal" is carried out involving the FIU, EIS, GPO, NSC, SRC, ARDFM, NB, STBs and other agencies and organizations. A total of 1,800 instances of issuing fictitious invoices were uncovered between 2017 and 7 months of 2022. The activities of 118 organized criminal groups were suppressed, 42 cases of laundering money derived from issuing fictitious invoices were detected. the number of convicted persons and case studies are given in the relevant sections of the IO.7

393. According to the competent authorities, the practical results of the "Stop-obnal" special operation include a 37% reduction in the amount of cash given out to legal persons, a twofold increase in the volume of non-cash transactions, a 16% increase in tax payments to the budget and a 9% reduction in the shadow economy.

394. To mitigate ML risks from customs offences and the cross-border movement of drugs, a special

operation named "Clean Customs" on the basis of a joint action plan of the FMA, NSC, MIA and SRC is being implemented. Within its framework 598 criminal offences in the customs sphere were revealed; smuggled goods to the amount of KZT 38,4 billion (more than USD 90 million) were seized; the activities of 13 organized groups, including 4 cross-border smuggling groups, were suppressed; 20 cases of smuggling involving customs officials were detected.

Case Study 7.14. Special operation "Clean customs"

The EIS, in cooperation with the FIU, suppressed the activities of an organized criminal group (OCG) engaged in economic smuggling. The case found that the OCG members organized the smuggling of cigarettes from the Islamic Republic of Iran through Aktau sea port under the guise of ceramic tiles and tomato paste. The task of the head of the customs post, O., according to his assigned role, was to release containers of contraband into free circulation without a customs inspection. The EIS detained and seized 30 containers that contained 21.5 million packs of cigarettes valued at approximately $4.6 million. The head of the OCG and a customs officer were sentenced by the court to 10 years in prison each and other members of the OCG to five years in prison. The smuggled goods were confiscated into the revenue of the state.

395. The country has provided case studies of the successful disruption of significant cross-border movements of narcotic drugs.

Case Study 7.15. Suppression of cross-border movement of drugs

The EIS received intelligence about the transit of a large consignment of Afghan heroin from Iran to the Federal Republic of Germany. In order to eliminate the heroin transportation channel, conducting a joint Police Intelligence Operation - controlled delivery - along the entire route was agreed upon with the competent authorities of Russia, Belarus, Lithuania, Poland, Germany, Luxembourg, Belgium and the Netherlands. Five trucks arrived across the Kazakhstan-Uzbekistan border into the territory of Kazakhstan. When placed under customs control procedures, the customs declaration reflected the delivery of goods (marble slabs) to a Kazakh company, which, in order to conceal the fact that the cargo was coming from Iran, made customs clearance of the export of goods to a Dutch company. During the customs inspection of one of the marble slabs, 2,210 briquettes of heroin were found and seized, the total weight of which was 1,105 kg and the value in the Western Europe shadow market amounted to USD 500 million and more. In order to identify the final recipients of the drug, 5 kg of heroin were placed in the cargo and it was transported from Kazakhstan via Russia, Belarus, Lithuania and Poland under the control of the competent authorities of foreign countries. Four members of the international criminal group (German nationals) were detained during the unloading of the goods in the territory of Germany and subsequently sentenced to imprisonment for a term of 3 to 6.5 years.

In the Republic of Kazakhstan, a pre-trial investigation into the smuggling of narcotic drugs was initiated, with deadlines interrupted due to the search for the suspect.

396. Measures taken as part of the "Clean Customs" special operation make it possible to minimize the risks of money laundering. Timely detection and suppression of smuggling of goods and narcotics, seizure and confiscation of smuggled items exclude the possibility of generating criminal income followed by its laundering.

397. The country provided case studies of the successful conduct of other special operations, such as "Kazyna" (identifying and combating the embezzlement of public funds), "Combating pyramid schemes" and "Barrel" (suppression of illicit trafficking in crude oil and petroleum products).

Case Study 7.16. ML from the embezzlement of the budget funds

On the basis of proactive information provided by the FIU, it was found that an organized criminal group under the leadership of P. carried out the construction of water wells for 300 peasant farms at the twice inflated price. The farmers were reimbursed at the expense of public funds. By accessing the bank

accounts of farms, subsidies received in the total amount of KZT 1 billion (more than USD 2 million) under the guise of legitimate transactions were transferred to the personal accounts of the criminal group members. The criminal proceeds were legalized by the members of the OCG through the purchase of expensive vehicles with their fictitious registration in the ownership of third parties. The criminal case on the fact of establishment and participation in an organized criminal group, theft and ML is under consideration in court.

Case Study 7.17. ML from illicit turnover of petroleum products

Citizen Zh., carrying out criminal activities in the sphere of illicit trafficking of petroleum products, on the basis of fictitious documents confirming the allegedly legal origin of fuels and lubricants, sold them in the territory of the Russian Federation to private individuals for a total of KZT 584 million (USD 1.8 million). The criminally obtained funds were legalized through the purchase of two petrol trucks, an industrial base with an administrative building, a land plot, five tanks for the storage of petroleum products, a railway dead end and warehouses under the guise of legal transactions for subsequent use in illegal business. The total value of the legalized property, which was seized during the pre-trial investigation, amounted to KZT 211 million (approx. USD 650 thousand).

The court found J. guilty of illicit trafficking in petroleum products, tax evasion and money laundering and sentenced him to imprisonment for a term of 5 years for the totality of the crimes committed. The legalized property was confiscated into the revenue of the state.

398. The data provided by country shows that the pre-trial investigative authorities sent cases of ML derived from all types of predicate offences and referred by the NRA to acts with a high ML risk for consideration on the merits in courts. Embezzlement accounted for 22.9% of the total number of ML cases considered by the courts, fraud - 16.3%, tax crimes (including issuing fictitious invoices) - 19.3%, economic crimes (illicit trafficking in crude oil and petroleum products, illegal gambling) - 19.9%, corruption crimes (abuse of power and bribery) - 11.4%, illicit drug trafficking - 6 %.

399. At the same time, there have been prosecutions and convictions for ML derived from theft (CC Article 188). According to the URPI, this type of offence accounted for 61% of the total number of offences in 2017 to 36% in 2021. The amount of property damage (i.e., potentially generated criminal income) resulting from theft is also significant. However, the NRA did not determine the degree of ML threat posed by this type of predicate offence. In addition, the number of MLs from illicit drug trafficking is insignificant (considering the total number of cases).

400. Thus, criminal statistical data and examples of detection, investigation and prosecution of ML cases generally correlate with the NRA in determining the types of predicate offences with high ML threat.

401. The state pursues the policy of combating the shadow economy, corruption, economic offences, tax and customs offences, and illicit trafficking in narcotic drugs and psychotropic substances. At the same time, the activities of the pre-trial investigative authorities are not limited to the detection and suppression of unlawful infringements. Significant efforts are made to prevent crime, reduce vulnerabilities and mitigate ML risks.

402. In this regard, the experts conclude that criminal persecution for ML is generally consistent with the nature of national threats and risks and national AML policies.

3.3.3. Types of ML cases pursued

403. The functions of criminal prosecution and administration of justice in the Republic of Kazakhstan are separate and autonomous. Trial courts, in accordance with their jurisdiction, consider the merits of criminal cases received after the pre-trial investigation and adopt the final procedural decision (a sentence of conviction or acquittal, a ruling to terminate proceedings). Revision of court decisions in criminal cases is carried out by higher courts on complaints of participants in the process or petitions (protests) of the

prosecutor.

404. The allocation of criminal cases to judges is done electronically based on experience, workload and specialization, which is determined by the type of predicate offences.

405. The "Torelik" information and analytical system of the judiciary authorities accumulates in online mode information on all procedural actions and decisions of judges in criminal proceedings. The system is integrated with information systems of LEAs/SSAs, including for the purposes of electronic proceedings in criminal cases, and compulsory enforcement agencies. The system contains a module of assistance to judges, which provides access to the necessary statutory documents and case materials.

406. Information on the number of ML cases received in court and considered on the merits broken down by predicate offences is shown in the table below (cases/persons).

Table 7.3. Breakdown of ML cases received in court and considered on the merits by predicate offence

Predicate offence	**2017**	**2018**	**2019**	**2020**	**2021**	**total**
Theft (CC Article 188)	2/2	-	1/1	1/1	-	4/4
Theft by misappropriation or embezzlement (CC Article 189)	3/3	10/10	7/8	12/20	6/6	38/47
Fraud (CC Article 190)	11/11	10/14	2/2	3/4	1/3	27/34
Extortion (CC Article 194)	-	1/3	-	-	-	1/3
Illicit trafficking in crude oil and petroleum products (CC Article 197)	2/2	6/9	3/3	2/2	3/3	16/19
Issuance of fictitious invoices (CC Article 216)	-	-	2/2	6/13	4/17	12/22
Production, storage or sale of counterfeit money (CC Article 231)	-	-	-	2/3	-	2/3
Tax evasion (CC Article 245)		7/7	2/7	4/8	4/8	20/33
Illicit drug trafficking (CC Article 297)	6/21	3/6	-	1/1	-	10/28
Illegal gambling operation (CC Article 307)	5/12	4/6	5/5	1/1	2/3	17/27
Abuse of power (CC Article 361)	-	12/15	1/7	-	1/1	14/23
Bribe-taking and bribe-giving (CC Articles 366, 367)	-	-	2/14	-	3/3	5/17
Total	32/54	53/70	25/49	32/53	24/34	166/260

407. The state prosecution in court proceedings is carried out by prosecutors (public prosecutors). If the public prosecutor discovers in court circumstances precluding criminal prosecution, he is obliged to declare a withdrawal of charges. Such a refusal entails the termination of the ML proceedings. There is no specialization of public prosecutors in ML cases. Representatives of the GPO stated that the complexity of a case and the experience of prosecutors are taken into account when entrusting the representation of the state in a prosecution. In complex and multi-count cases, the state prosecution functions may be assigned to a group of public prosecutors. In addition, the state prosecution may be entrusted to procedural prosecutors who supervise the legality of pre-trial investigations.

408. The statistical data and case studies provided show that the courts considered the merits of ML criminal cases for various categories of predicate offences. The main method of ML in the cases considered was self-laundering, however, the courts have also considered criminal cases of ML by third parties, including professional launderers, ML in the Republic of Kazakhstan when the predicate offence was begun abroad (see case studies above).

409. There were facts of pre-trial investigation of ML without a predicate offence, but subsequently, the persons were either charged for ML in conjunction with the predicate offence, or the criminal prosecution under Article 218 of the CC was terminated. In this regard, there have been no such cases in judicial practice. Since such cases were not sent to court by the criminal prosecution authorities, they were not considered by the courts.

Table 7.4. Statistical data of the SC on the results of consideration of ML criminal cases (by the number of cases/persons).

	2017	**2018**	**2019**	**2020**	**2021**	**total**
Total number of ML and predicate offence cases against persons	32/54	53/70	25/49	32/53	24/34	166/260

Convicted of ML and predicate offence	25/39	35/39	14/19	19/31	13/15	106/143
Acquitted for ML with conviction of a predicate offence	5/6	7/15	5/24	3/5	11/19	31/69
Prosecution for ML was terminated on exonerative grounds (including due to withdrawal of charges by public prosecutor) with conviction of a predicate offence	2/9	11/16	6/6	10/17	-	29/48

410. The above statistical data shows that in 63.8% of cases the courts issued guilty verdicts in ML cases. In 18.7% of cases, acquittals were issued, and in 17.5% of cases, proceedings were terminated on rehabilitative grounds (denial of prosecution by state prosecutors). There were no facts of acquittal or termination of proceedings to the full extent of the charges; all persons were convicted of predicate crimes. In comparison with the significant increase in acquittals in criminal cases of predicate offences with the full acquittal of charges (2016 - 62, 2017 - 70, 2018 - 270, 2019 - 318, 2020 - 329, 2021 - 272), the dynamics of convictions for ML offences are stable.

411. The analysis of the acquittal judicial decisions submitted by the country found that, as a rule, public prosecutors and courts did not question the correctness of the establishment at the pre-trial stage of the factual circumstances of the criminal case, the completeness and comprehensiveness of the investigation into the fact of receipt of criminal income and the method of its introduction into the legal circulation. At the same time, the qualification of actions for the disposal of property as ML was excluded as unnecessary due to the court's conclusion that the offenders had no special purpose of concealing its criminal origin.

Case Study 7.18. Exclusion of the ML charge

During the pre-trial investigation into the criminal case against two officers of the interregional department of the internal affairs body for combating illicit drug trafficking, the NSC found that acting by prior agreement between themselves, they carried out an illegal search in the house of the individual A., during which they found and appropriated 1 kg of heroin. For not prosecuting A. for drug possession, the offenders demanded a bribe of USD 50 thousand. After receiving the bribe in cash, B. transferred the money to his personal bank account. Since he did not take any steps to conceal the criminal origin of the money, the public prosecutor withdrew the charges against B. for ML, and therefore the court decided to terminate criminal prosecution under CC Article 218. As to the rest of the charges against B., he was found guilty and convicted.

412. Most often acquittal decisions were made in criminal cases of theft - 31 persons, or 26.5% of the total number, and corruption crimes (bribe-taking) - 20, or 17.1 %.

413. The mere existence of acquittal decisions in ML cases is not considered by experts as a negative factor in assessing the activities of pre-trial investigation bodies, since the reason for such decisions was not violations of the law during the collection of evidence, its falsification, or incomplete investigative actions. The facts of acquittal of persons and withdrawal of charges by public prosecutors indicate a certain degree of independence and impartiality of the judicial system, objectivity of public prosecutors, as well as the formation of judicial practice in ML cases as defined in international anti-money laundering regulations.

414. In 2019, a Commission was established in the GPO, which is responsible for assessing the quality of the investigation and prosecutorial supervision of each acquittal decision, establishing the causes and conditions that led to acquittal and making recommendations to prevent them in the future. Analysis of the reasons for acquittal is brought to the LEAs and SSAs. Thus, the country undertook practical measures to form a uniform law enforcement practice and eliminate the facts of unjustified criminal prosecution for ML.

415. This approach allows for the timely identification of acquittals that are not well justified.. According to the GPO, the acquittals of three persons were overturned on protest by prosecutors, with their subsequent conviction for ML.

Case 7.19. Cancellation of acquittal in ML case

By a court verdict, D. was convicted under CC Articles 216 and 245 (invoicing without actually

performing work or providing services, large-scale tax evasion) to five years imprisonment with probation. She was acquitted under articles 218 and 262 of the CC (money laundering and organisation and management of an organised criminal group). The prosecuting authority accused D. of legalising the criminal proceeds from tax evasion and fictitious invoices by acquiring two properties and fictitiously registering them as the property of a third party. The court's finding of not proving guilt in the ML part was unmotivated and made without a full and comprehensive assessment of the evidence presented. The verdict was quashed on appeal by the prosecutor and the case was remitted for a new trial. As a result, D. was sentenced to seven years imprisonment for the cumulative offences, including ML.

Table 7.5. Number of convictions for ML by predicate offenses.

Predicate offence	2017	2018	2019	2020	2021	total
Theft (CC Article 188)	-	-	1	1	-	2
Theft by misappropriation and embezzlement (CC Article 189)	3	5	8	7	1	24
Fraud (CC Article 190)	11	11	2	3	-	27
Illicit trafficking in crude oil and petroleum products (CC Article 197)	2	9	3	2	3	19
Issuance of fictitious invoices (CC Article 216)	-	-	1	7	3	11
Production, storage or sale of counterfeit money (CC Article 231)	-	-	-	3	-	3
Tax evasion (CC Article 245)	2	6	2	8	5	23
Illicit drug trafficking (CC Article 297)	12	3	-	-	-	15
Illegal gambling operation (CC Article 307)	9	2	-	-	2	13
Abuse of power (CC Article 361)	-	3	-	-	-	3
Bribe-taking and bribe-giving (CC Articles 366, 367)	-	-	2	-	1	3
Total	39	39	19	31	15	143

416. According to court statistics, out of a total of convictions for ML, the most common is a conviction for ML derived from stealing of property (CC Articles 188-190) - 53 persons, or 37%, tax evasion - 23 or 16%, illicit trafficking in crude oil and petroleum products - 19 or 13.3%, illicit drug trafficking - 15 or 10.5%, organization of illegal gambling business - 13 or 9%, which correlates with the NRA findings about the definition of these predicate crimes as high ML threats.

Case Study 7.20. ML from illegal gambling business

The FIU detected suspicious financial transactions for cashing out funds from the account of a legal person in large amounts. The bank transactions were suspended by the FIU, and the relevant information was sent to the EIS. During the pre-trial investigation, it was found that individuals Or. and O. and other persons organized illegal gambling business in the form of online gambling using the Internet (electronic casino). The proceeds of crime (amounting to more than KZT 5.3 billion or USD 13.8 million) were cashed out and transferred to the bank accounts of close relatives of criminals in order to legalize and introduce them into legal circulation. Court ordered to seize funds in banks to the total amount of KZT 580.2 million, as well as movable and immovable property acquired with the proceeds of crime (a parking lot in Astana, 5 cars of elite brands).

The court sentenced the offenders for the totality of the crimes committed under CC Articles 307 and 218 to imprisonment for a term of 4 years with confiscation of the criminal income and property acquired with the proceeds of crime in the amount of over KZT 780 million (over USD 1.8 million).

417. A fairly common offence in the Republic of Kazakhstan is the issuance of invoices without the actual performance of work, provision of services and shipment of goods. In 2017-2021, 1,602 offences of this category were detected. For these purposes, offenders establish shell companies that facilitate tax evasion and embezzlement of public funds by issuing fictitious invoices. Monetary funds are cashed out in order to introduce them into legal circulation. Being, in fact, a form of professional ML, such illegal activities are often committed by organized groups and pose a significant threat to national economic security. Kazakhstan provided case studies of successful prosecutions for these activities, as well as identification of

ML associated with this type of illegal activity.

Case Study 7.21. Issue of false invoices and ML

In cooperation with the FIU, the EIS suppressed the activities of an organized criminal group under the direction of individual P. In order to assist in the laundering of criminal income, a criminal group created 29 shell companies, on behalf of which invoices were issued without actually performing work, providing services or shipping goods. Turkish national E., using fictitious invoices, avoided paying taxes on a particularly large scale and cashed out more than KZT 2 billion over the period 2015-2019, part of which he converted into USD 2.1 million and withdrew the amount to his bank account in Turkey. With the legalized criminal proceeds E. purchased 4 real estate objects and 4 cars.

The court convicted P. and 7 members of the organized group for establishing and participating in such a group, tax evasion and issuing fictitious invoices to various terms of imprisonment. E. was found guilty of tax evasion and money laundering and sentenced to imprisonment for a term of 7 years with confiscation of property acquired with the criminally obtained funds in the total amount of KZT 250 million (approx. USD 600 thousand).

418. The country provided cases of ML by third parties. There have been instances where organized criminal groups have involved individuals with specialized skills in certain areas, whose role has been solely to launder the proceeds of crime. While not directly related to the commission of the predicate offence and the proceeds of crime, such persons, acting as professional launderers, ensured that the proceeds of crime were laundered legally.

Case Study 7.22. ML by third parties with signs of professional laundering

A transnational criminal organization comprised of five Kazakh citizens was detected and suppressed by the NSC, which was involved in the illegal sale of narcotic drugs and psychotropic substances. Each of the members of this organization performed the role assigned to them by the organizers in the commission of a crime, including the purchase of psychoactive substances in especially large quantities, their packing into smaller wholesale lots, smuggling of precursors, maintenance of a chemical laboratory, manufacturing, transportation, storage and distribution to end users. Yu, who had skills in the IT sphere, was involved in the activities of the criminal organization with the sole purpose of the laundering of criminal income. For this purpose, Yu recruited persons, who were unaware of the crime being committed and gave him access to their bank cards through an Internet application for a fee. Bank card details were published on the Internet and funds were transferred to them from drug buyers. By remotely accessing the bank transactions, Yu converted the funds into bitcoins and transferred them to anonymous electronic crypto accounts of the leaders of the transnational criminal organization. The total amount of criminal proceeds legalized by Yu was over $2.1 million.

The court found Yu guilty of participating in a criminal organization and money laundering and sentenced him to nine years imprisonment as a set of crimes. Other members of the criminal organization were convicted of participation in it, smuggling, and illicit drug trafficking to long terms of imprisonment.

419. It should be noted that the above case also established the transnational nature of the predicate crime. One of the organizers and leaders of the criminal organization was a citizen of the Russian Federation, who involved citizens of Kazakhstan, including Yu, in the commission of the crime as a structural unit of a transnational criminal organization. Narcotic drugs, psychotropic substances, precursors, chemical liquids and laboratory utensils came from the Russian Federation, including through smuggling, and the sale of psychoactive substances and ML were conducted in the territory of Kazakhstan. Thus, the predicate crime started in a foreign jurisdiction and ended in Kazakhstan, and the laundering of criminal proceeds took place in Kazakhstan.

420. The judicial system of the Republic of Kazakhstan has demonstrated the availability of adequate

human and material-technical resources, allowing for judicial hearings of different types of ML.

421. Representatives of the competent authorities and the court did not mention any aspects of the investigative, prosecutorial or judicial process that hindered or delayed the prosecution and sanctioning of ML. No such factors were identified by the experts either.

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

422. According to the CC, ML is classified as a serious offence[16]. The disposition of CC Article 218 provides for three parts and establishes a gradation of liability depending on the qualifying factors of the offence (detailed in R.3).

423. A comparative analysis of sanctions for predicate offences and ML classified by the CC as economic offences showed that the category of grave offences includes especially aggravated offences, i.e. offences committed by a criminal group or involving damage on a particularly large scale, for instance, CC Article 216(3) (invoicing), CC Article 217(3) (creation and management of a pyramid scheme), CC Article 234(3) (economic smuggling), CC Article 245(3) (tax evasion by corporate entities). The offences stipulated by Parts 1 and 2 of the above CC articles fall under the category of minor or medium gravity.

424. Accordingly, the liability for ML offences is stricter than for other economic offences.

425. Punishment shall be inflicted by courts taking into account the nature and degree of public danger of a criminal offence, the personal background of a guilty person and circumstances, which aggravate and mitigate liability.

426. According to the information provided by the country, in the assessed period, persons were convicted for ML only in the aggregate with predicate offences. According to the rules established by CC Article 58(1), in this situation, the court imposes punishment for each offence included in the aggregate of offences and then determines the final punishment by absorbing the less severe punishment by the more severe one or by adding them together in full or in part. Additional punishments (confiscation of property, deprivation of rank, deprivation of the right to hold certain positions, etc.) are added to the final primary punishment.

Table 7.6. Statistical information on sentences imposed on persons convicted under CC Article 218 in the aggregate with predicate offences .

Convicted persons		**2017**	**2018**	**2019**	**2020**	**2021**	**total**
total		39	39	19	31	15	143
primary punishment							
imprisonment		32	34	17	29	15	127
for a term of	up to 3 years	11	6	4	3	4	28
	3 to 6 years	8	13	4	14	2	41
	6 to 10 years	8	12	7	10	7	44
	more than 10 years	5	3	2	2	2	14
from imprisonment under Article 63 of the CC (probation)		2	7	3	2	1	15
applying Article 55 of the CC		1	3	-	-	-	4
fine		-	2	-	-	-	2
restriction of freedom		7	3	2	2	-	14
additional punishment							
confiscation of property		18	12	6	4	8	48
deprivation of special or military rank		-	-	1	-	-	1
deprivation of the right to hold certain positions		16	17	13	9	1	56
deportation of a foreigner from the Republic of Kazakhstan		-	-	-	1	-	1

427. It follows from the above data that the predominant type of punishment is the most severe one - imprisonment, which accounted for 88.8% of the total number of offences. 10.5% of persons sentenced to imprisonment are under probation (in this case the punishment is not served, and the person is under the

[16] Before the amendments to the Criminal Code made by Law No. 131-VII dated July 1, 2022, the offence under CC Article 218(1) was classified as a crime of medium gravity.

probationary control of the authorized state body, performing the duties imposed by the court for a period of time determined by the court). Milder types of punishment - restriction of freedom and fines - were imposed on 9.8% and 1.4% of convicted persons, respectively. Additional punishment in the form of confiscation of property was imposed on 33,6% of convicted persons, deprivation of the right to hold certain positions or engage in certain activities - 39.2%.

428. The term of the final sentence is more influenced by the punishment for the predicate offence, since the courts' practice has been to impose a stricter sentence for the predicate offence, with the final sentence determined by absorbing the punishment for ML.

Case Study 7.23. Sentencing for ML in conjunction with a predicate offence

The court found K. guilty of establishing and participating in an organized group (CC Article 262(1,2) - serious crime), making arrangements for issuing fictitious invoices by a criminal group (CC Article 216(3) - serious crime), large-scale money laundering (CC Article 218(3), Par. 2, 3 - serious crime).

She was sentenced to imprisonment with confiscation of property under Article 262(1) for a term of 7 years, under CC Article 262(2) for a term of 5 years and under CC Article 216(3) and CC Article 218(3) (for each of the charges) for a term of 3 years and 6 months.

She was finally sentenced to imprisonment for a term of 7 years with confiscation of property by absorption of the less strict sentence with the more strict one.

429. According to the country's information, there were no cases of committing ML by persons previously convicted under CC Article 218, which indicates that sanctions against natural persons are dissuasive and ensure the fulfilment of the function of private prevention.

430. Thus, taking into account the differentiation of liability for ML offences established by law, the absence of special repetition of offences and the practice of sentencing, including additional punishments, the experts conclude that sanctions for ML are applied to physical persons and are proportionate, dissuasive and effective.

431. The criminal liability of legal persons for ML is not established in accordance with the fundamental principles of national legislation. Administrative liability of legal persons for ML in 2017-2021 was also not provided.[17] There are no examples of the application of liquidation to legal persons for ML in accordance with the norms of civil law. Therefore, no sanctions were applied to legal persons for ML offences in the assessed period. At the same time, the lack of sanctions for legal persons is not considered by experts to be a significant disadvantage, because while their use in the commission of predicate offenses is widespread, the practice of using legal persons in ML is not significant.

3.3.5. Use of alternative measures

432. The competent authorities indicated that if the ML elements are not proven, there is prosecution and conviction for the predicate offence (e.g. fictitious invoicing, tax crimes, theft, corruption offences). Relevant statistics are provided in Core Issue 7.3.

433. The unauthorized purchase or sale of property knowingly obtained by criminal means without indicators of ML entails criminal liability under CC Article 196. The most strict punishment for such actions committed by an organized group or by a person exercising the powers vested in him by virtue of his office is imprisonment for a term of up to 5 years with confiscation of property. In 2017-2021, pre-trial investigations were initiated for almost 1.4 thousand offences under CC Article 196.

434. In cases where it is impossible to secure a conviction for money laundering because a person is internationally wanted, or when proceedings are terminated for reasons other than exoneration (amnesty, expiration of the limitation period for criminal liability, death of a suspect), the institution of non-

[17] Administrative liability of legal persons for ML (CAO Article 214-1) was established by Law No. 132-VII dated July 1, 2022, which entered into force on September 5, 2022.

conviction-based (pre-trial) confiscation of criminal property may be applied.

435. In such situations, the person conducting the pre-trial investigation separates materials for pre-trial confiscation, which are sent to the prosecutor. The decision on confiscation is taken by the court on the basis of the prosecutor's request.

436. Over the period from 2018 (from the moment of introduction of pre-trial confiscation) to 7 months of 2022, the courts satisfied 17 prosecutors' requests for pre-trial confiscation in the amount of KZT 9.8 billion (more than USD 23 mln).

437. See IO.8 for case studies of the application of pre-trial confiscation in ML cases.

438. Thus, when it is not possible to secure a conviction for ML, the country applies alternative measures.

Overall conclusion on IO.7

439. The powers of pre-trial investigative authorities to detect, suppress and investigate ML crimes are implemented in accordance with the legislation of the Kazakhstan and taking into account the specific anti-crime tasks performed by each agency within its purview. In general, this work is carried out in a systematic manner.

440. The competent authorities have the necessary human, information and analytical resources. The "follow the money" principle is consistently implemented in the country, measures have been taken to improve the methodology of parallel financial investigations, access to a wide range of necessary financial information is provided. The level of interagency cooperation is high. International cooperation mechanisms are used for the purpose of combating crime in general and ML in particular.

441. The detected, investigated and prosecuted ML types are generally consistent with the nature of national threats and risks and national AML policy.

442. Natural persons convicted of ML offences are subject to proportionate, dissuasive and effective sanctions. No sanctions have been imposed on legal persons for ML in the country.

443. If it is not possible to secure a conviction for ML, a criminal prosecution for the predicate offence is carried out. In cases prescribed by law, the institution of non-conviction-based (pre-trial) confiscation is applied.

444. **Kazakhstan is rated as having a substantial level of effectiveness for IO.7.**

3.4. Immediate Outcome 8 (Confiscation)

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

445. Confiscation of the proceeds, instrumentalities and means of crime is one of the priority areas of government policy in the fight against crime. Measures to improve national legislation on the legal regulation of the institution of confiscation and to ensure the effectiveness of the work of the competent authorities to search for and confiscate property obtained by criminal means are contained in the strategic policy documents on legal policy concepts for 2010-2020 and 2020-2030, which were approved by Decrees of the President of Kazakhstan dated 24 August 2009 and 15 October 2021.

446. As part of the implementation of these Concepts, national legislation has been amended, in particular, confiscation of property as an additional punishment has been introduced as a sanction for all predicate offences classified as established offences by the FATF Methodology, and the institution of pre-trial confiscation has been established.[18]

[18] Confiscation of property was not envisaged as an additional punishment for the intentional infliction of grievous bodily harm for selfish motives or for hire under CC Article 106(2), Par. 6; illegal actions with regard to insider information and manipulation of the securities market, which caused damage on a large scale (Part 1 of CC Articles 229, 230); evasion of taxes and customs duties (CC Articles 236, 244 and 245); acquisition or sale of property knowingly obtained by criminal means, including repeatedly (CC Article 196(1,2); trafficking in arms (CC Article 287); forgery and sale of forged documents (CC Article 385); and organization of illegal migration (CC Article 394).

447. The procedural obligations and powers of the prosecuting authorities to take measures to identify property obtained in a criminal way or acquired with criminal proceeds, instrumentalities and means of committing an offence are duly regulated by the law of criminal procedure (for more details see Recommendation 4).

448. The Prosecutor General of the Republic of Kazakhstan issued regulatory Instructions dated 30.05.2019 "On intensification of activities to recover damages caused by criminal offences", dated 15.09.2021 "On strengthening the organisation of work against legalisation (laundering) of property obtained by criminal means, activation of parallel financial investigations", obliging all criminal prosecution bodies to carry out tasks of identification, search, confiscation and return of criminal assets. A unified methodology has been developed for conducting parallel financial investigations.

449. The performance of the competent authorities in conducting parallel financial investigations, identifying and seizing assets, and recovering and confiscating damages is considered a criterion for their effectiveness. The said activities are analysed on an ongoing basis. The experts were familiar with both intradepartmental and interdepartmental regulations (in particular, decisions of the board of the Prosecutor General's Office of the RK, the Coordination Council of the RK on ensuring law and order and combating crime and others) containing specific instructions and organisational and practical measures to ensure confiscation and reparation of damages.

450. Thus, a comprehensive analysis of the legal regulation and application of confiscation shows that, in the RK legislation this institution is considered as a consequence of a criminal offence and is a means of implementing the state criminal law policy in the sphere of combating and preventing crime. The application of confiscation is ensured by the government authorities, which are vested with the relevant powers.

451. Outside of criminal proceedings (e.g. - confiscation of unconfirmed income of public officials under anti-corruption laws), confiscation does not apply.

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

452. Statistical information on the amount of damage caused by predicate offences is provided in the table below.

Table 8.1. Amount of damages caused by predicate offences (USD mln.)

Year	Amount of damages	Compensated damages during pre-trial investigation in the amount of	% of the amount of damages	Seized and confiscated property in the amount of	% of the amount to be recovered [19]
2017	965,3	374,6	38,8	125,7	21,3
2018	688,4	348,4	50,6	185,4	46,4
2019	816	320	39,2	112,9	22,8
2020	1 657,9	400,1	24,1	290	23
2021	709,4	150,7	21,2	76,1	13,6
Total	4 837,2	1 593,9	32,9	790,2	24,4

453. Rather high amounts of voluntary compensation for damage during pre-trial proceedings are due to the norms of the criminal law, stimulating positive post-criminal behaviour of guilty persons. In particular, voluntary compensation of damages is the basis for exemption from criminal liability for a number of economic offences, including tax crimes.

454. According to the tax authorities, more than USD 2 billion in additional taxes have been assessed as a result of tax compliance audits. Revenue from taxes and levies to the budget increased by 16% in the period under review.

455. Voluntary payment of damages in criminal proceedings is regarded as a ground for mitigating liability

[19] The amount to be recovered is the amount of the damage caused after deduction of the amount of voluntary compensation

and is the basis for imposing a penalty not involving actual deprivation of liberty.

Case Study 8.1. Voluntary restitution (criminal income)

Director of a public utility company providing water supply services to the population, by drawing up fictitious contracts stole money from the enterprise in the amount of KZT 126.2 million (approx. USD 300 thousand). He also set monopoly high prices for socially important services, as a result of which he obtained criminal income on a large scale (over USD 860 thousand). A. legalized the criminally obtained funds under the guise of legal investment in the development of hotel business.

Based on the investigation findings, a temporary compensatory tariff was set to reduce by 54.4% the payment for water supply to a number of settlements for a period of 1 year. The damage caused by the crime (taking into account the temporary compensatory tariff) in the amount of more than USD 1.1 million was fully reimbursed by the offender.

A. was convicted of theft by misappropriation, monopoly activities and laundering of criminal proceeds and sentenced to imprisonment for a term of 6 years for the totality of the crimes committed.

456. The effectiveness of pre-trial investigative authorities in taking provisional measures for the confiscation of property and compensation for damages is relatively not high. During this period, the property was arrested and seized for 24,4% of the amount to be recovered. The above indicates that the efforts to identify and locate property subject to seizure should be intensified.

457. Based on the information provided by the pre-trial investigative authorities, the effectiveness of their seizure activities in ML cases is slightly higher. In particular, in cases of ML offences (in the aggregate with predicate offences) investigated by the EIS, the value of property seized during pre-trial proceedings was 57.3% of the amount of damages.

458. During the on-site mission, pre-trial investigative explained that the amounts of property seized are generally reflected in statistical cards for predicate offences. Centralised records of property value, seized in ML cases, broken down by predicate offences and the amount of income generated by predicate offences are not kept.[20] Analytical information provided by the agencies on property seizure in ML cases is fragmented. Due to deficiencies in statistical records, it was not possible to draw definitive conclusions about the effectiveness of pre-trial investigative authorities in identifying and seizing property in ML cases.

459. In fulfilling their procedural obligations to enforce the sentence in terms of property confiscation and other property penalties, the pre-trial investigative authorities conduct parallel financial investigations in the course of the CIDA and pre-trial investigation in order to find the property subject to seizure. The procedure for their conduct, goals and objectives, including the establishment of the movement of criminal proceeds, the relationship between the source of origin and recipients of funds, other property obtained by criminal means, the circumstances of the acquisition of the assets, their location, the return and confiscation of criminal assets are regulated in detail by the Methodological Recommendations developed jointly by the FMA and GPO and binding for all LEAs/SSAs.

460. As part of parallel financial investigations, the competent authorities, in order to identify a criminally obtained property, carry out activities aimed at verifying a wide range of information, including from open sources, information databases of government authorities, organizations, institutions, as well as information on suspicious transactions received from non-government organizations and institutions.

461. There are case studies of successful parallel financial investigations that have uncovered a significant amount of property to be seized and confiscated.

Case Study 8.2. Parallel financial investigation to ensure confiscation

[20] The concepts of "criminal damage" and "criminal proceeds" are not identical. All predicate offences generate criminal proceeds, but they may not involve material damage (for example, in drug trafficking, the perpetrator profits from the sale of illegal substances, but the cost to the drug user of purchasing them is not considered to be damage due to the illegality of the transaction).

The EIS conducted a pre-trial investigation into the criminal case against R. on the theft of public funds on an especially large scale and found that the criminal proceeds were legalized by the offender by purchasing immovable property (two residential buildings, a commercial facility, an industrial facility) and two cars under the guise of legal transactions. During the parallel financial investigation, the criminal property was seized.

The court found R. guilty of theft by misappropriation, embezzlement and fraud on an especially large scale and ML of criminal proceeds and sentenced him to imprisonment for a term of 7 years and 6 months. The criminal property worth KZT 56 million (more than USD 150 thousand) was confiscated.

462. The effectiveness of parallel financial investigations is enhanced by the establishment of special units within the EIS and ACA, which are exclusively responsible for conducting such investigations. Officers of such units are included in operational investigative groups. Prior to the establishment of these units, specialists from other government authorities and organizations, who analyzed all available information for the purpose of identifying criminally obtained property, were included in the operational investigative groups for the purpose of conducting parallel financial investigations.

Case Study 8.3. Participation of specialists in a parallel financial investigation

During the investigation into the criminal case on the theft of public funds in an especially large amount by T., the ex-head of the national company "Astana-Expo-2017", the ACA operational investigative group included the officers of the mentioned company, who were exclusively engaged in the search of criminal property. As a result, the following property purchased with criminally obtained funds was found and seized: apartments, land plots, shares in the authorized capital of enterprises, money in bank accounts and 6 cars. The total value of the seized property amounted to KZT 18.4 billion (over USD 56 million). Upon conviction, the confiscated property was used to compensate for the damage caused by the crimes.

463. Other case studies of successful parallel financial investigations are provided in IO.7.

464. According to the information provided by the competent authorities, one of the main ML typologies is the acquisition of property with criminally obtained funds and fictitious registration as the property of third parties. According to the explanations provided in Par. 20 of SC Regulatory Resolution No. 4 on Certain Issues of Criminal Sentencing dated June 25, 2015, confiscation of property registered in the name of third parties may be applied, provided that its criminal origin is proven. Having access to a wide range of financial information and making effective use of information and analytical resources (for more details, see IO.7), pre-trial investigative authorities in parallel financial investigations identify and prove facts of fictitious registration of criminal property or property purchased with criminally obtained funds into the ownership of third parties, and the courts confiscate such property.

Case Study 8.4. Confiscation of property fictitiously registered to third parties

During the pre-trial investigation into the criminal case against R., who committed theft by misappropriation and fraud, it was found that with the criminally obtained funds the offender purchased a house with outbuildings and a land plot, as well as a commercial facility (store). With a view to conceal the criminal origin of this property, it was fictitiously registered in the name of his wife R., and then on the basis of a sales contract, it was transferred to her close relative without the intention of actual alienation. A parallel financial investigation proved the purchase of this property with criminally obtained funds, as well as the fictitiousness of transactions to register it as the property of third parties.

R. was convicted by the court for theft of property and laundering of criminal proceeds and sentenced to imprisonment for a term of 8 years. The real estate objects (the house, the store and the land plots) were confiscated.

465. The legislation establishes mechanisms to protect the rights of bona fide third parties. Based on the

above regulatory resolution of the SC, the lack of awareness of the property owner (third party) about the criminal origin of the property or about the unlawful purposes of its use excludes the application of confiscation. In such cases, the courts decide on confiscation of a sum of money equivalent to the value of the property subject to confiscation.

Case Study 8.5. Confiscation of value equivalent

In a criminal case against O. on the fact of organizing an illegal gambling business and money laundering, it was found that one of the cars purchased with criminally obtained funds, was sold to S., who was a bona fide purchaser of the property and was not aware of the criminal origin of this property. The court decided to release the car from seizure, leaving it in the possession of S., and to confiscate the sum of money equivalent to its value from the offender.

466. Despite the fact that the competent authorities have recorded the facts of receiving criminal proceeds or their transformation into virtual assets, practical mechanisms for the seizure of crypto assets involve only the voluntary provision to the pre-trial investigative authority of access to crypto wallets by defendants in criminal cases. However, this deficiency is compensated to a certain extent by the confiscation of a sum of money corresponding to the value of the criminally obtained property.

Case Study 8.6. Confiscation of value equivalent

As part of a pre-trial investigation into a criminal case of illicit drug trafficking, the NSC operational investigative group found that the criminal proceeds were transferred to a professional launderer Yu., who accumulated it through drop cards and subsequently purchased cryptocurrency. The amount of legalized money was over KZT 873 million (USD 2.1 million). Yu. provided the pre-trial investigative authority with access to the crypto wallet for the purpose of converting virtual assets into fiat money and subsequent seizure. However, at the time of the investigation, the cryptocurrency had been transferred to another cryptocurrency account by other members of the transnational drug network who had access to the crypto wallet.

The court convicted Yu. for money laundering and participation in the activities of a criminal organisation and sentenced him to imprisonment. The amount of property legalised was recovered from him to the state.

Case Study 8.7. Withdrawal of VAs

In the course of the "control purchase" intelligence operation with the participation of suspect I., a purchase of a large batch of narcotic drugs was carried out. The payment received in bitcoins was cashed by I. under the control of the NSC in one of the crypto exchanges, the money in the amount of KZT 70 million (over USD 150 thousand) was seized. The investigation into the case continues.

467. The country takes measures to prevent the transfer of assets to foreign jurisdictions, to identify and seize criminal assets abroad and to return such assets. The relevant action plan approved by the Deputy Prime Minister of Kazakhstan on June 28, 2022, includes a wide range of measures for suppressing the withdrawal of criminal capital abroad and returning funds to the country, increasing the effectiveness of the competent authorities' efforts. These measures are implemented in cooperation with the GPO, NB, ARDFM, MoF, FMA, ACA, MIA and NSC.

468. For the purpose of identifying property and bank accounts abroad, the pre-trial investigative authorities send international investigative requests to identify and seize such property. Case studies are provided of successful identification and return of assets moved to foreign jurisdictions, however, the statistics were not provided.

Case Study 8.8. Asset recovery from abroad

The ACA has a criminal case in charge against a member of the criminal community M. suspected of establishing and directing an organized criminal group, economic smuggling and ML. It was found that M., who is internationally wanted, legalized part of the criminal proceeds of the criminal community by withdrawing criminal assets in the amount of USD 1.3 million and transferring the money to a bank account in the European state. The RK court granted the prosecutor's request for pre-trial confiscation of these funds. On the basis of the court decision, the European state federal authorities returned to Kazakhstan USD 1.3 million credited to the state budget.

469. The GPO takes measures to improve the effectiveness of pre-trial investigative authorities in the field of international cooperation in general and in the identification and return of property moved to foreign jurisdictions. For these purposes, an algorithm of actions of competent authorities for the organization of international cooperation was developed, requirements for the execution of requests for mutual legal assistance were established and a methodology for the search and seizure of criminal assets abroad was drawn up.

470. Officers of all LEAs/SSAs participated in training activities aimed at improving their skills in identifying property subject to confiscation, including abroad, and taking provisional measures. The training and methodological programs provided to the experts by the departmental training and scientific institutions include relevant courses for the training staff.

471. Practical aspects of LEAs/SSAs' activities are used for the purpose of improving national legislation on the application of confiscation. Since 2018, the institution of pre-trial (non-conviction-based) confiscation has been applied in the country. In total, during this period (including 7 months of 2022) the courts granted 17 prosecutors' requests for pre-trial confiscation in the amount of KZT 9.8 billion (over USD 23 million).

Case Study 8.9. Pre-trial confiscation of proceeds of crime held abroad

The NSC investigation into the criminal case against T. for large-scale embezzlement, tax evasion, forgery and use of knowingly false documents, establishment and direction of an organized criminal group found that the criminal proceeds were legalized by withdrawing assets through controlled legal persons and crediting them to the European bank accounts.

T. was put on an international wanted list. At the request of the RK GPO, the European state’s prosecutor's office blocked USD 13 million in T.'s bank accounts. The RK court granted the prosecutor's request for pre-trial confiscation of these funds. At present, the RK competent authorities are enforcing the court decision and taking steps to return the assets from the European state as part of MLA.

Case Study 8.10. Pre-trial confiscation of proceeds of crime held abroad

In the criminal case under investigation by the NSC on the fact of organization of illegal gambling business, tax evasion, and ML, 5 suspects were put on the international wanted list. The court satisfied the prosecutor's request for pre-trial confiscation of criminally obtained property of the suspects, namely funds in bank accounts and money seized during the search in the amount of over KZT 465 million (USD 1.1 million), USD 6 million, EUR 793 thousand, 3 cars and 4 aircraft.

Besides that, by sending an international investigative order, it was established that one of the suspects had purchased three apartments in the territory of the state R. with the criminally obtained funds. At the request of the prosecutor, the RK court decided on their pre-trial confiscation. At present, the court decision is being executed as part of MLA.

472. In 2017-2021, the number of individuals convicted of ML offences in the aggregate with predicate offences, with courts applying confiscation of property as an additional punishment, was 48 or 33,6% of the total number of individuals convicted of ML.

Table 8.3. Number of persons convicted of ML in combination with the predicate offences with confiscation (convicted persons/ of them with confiscation)

Predicate crime	2017	2018	2019	2020	2021	Total
Theft (ст.188 CC)	-	-	1/1	1/0	-	2/1
Embezzlement or misappropriation of the property (ст.189 CC)	3/0	5/2	8/2	7/2	1/1	24/7
Fraud (ст.190 CC)	11/5	11/4	2/1	3/1	-	27/11
Illicit trafficking in oil and petroleum products (ст.197 CC)	2/2	9/1	3/0	2/0	3/0	19/3
Illegal invoicing (ст.216 CC)	-	-	1/1	7/1	3/3	11/5
Counterfeiting (ст.231 CC)	-	-	-	3/0	-	3/0
Tax evasion (ст.245 CC)	2/0	6/1	2/0	8/0	5/2	23/3
Illicit drugs trafficking (ст.297 CC)	12/4	3/1	-	-	-	15/5
Organization of illegal gambling business (ст.307 CC)	9/7	2/2	-	-	2/2	13/11
Abuse of power (ст.361 CC)	-	3/1	-	-	-	3/1
Taking and giving a bribe (ст.ст.366, 367 CC)	-	-	2/1	-	1/0	3/1
Total	39/18	39/12	19/6	31/4	15/8	143/48

473. According to the information provided by the SC, in criminal cases on ML offences (in the aggregate with predicate offences), the subject of confiscation were vehicles (73), real estate objects (68), money worth over 1.2 million USD (in equivalent), shares in the authorized capital of legal persons (4) and other property.

474. No statistics have been provided on the types of confiscation (property obtained by criminal means or purchased with criminally obtained funds, instrumentalities of crime, monetary equivalent. However, examples are provided of the use of confiscation of instruments and means of crime, and of the equivalent of money.

Case Study 8.11. Recovery of the value equivalent of the proceeds of crime

A court convicted members of a transnational organised group to long prison terms for trafficking in narcotic drugs, psychotropic substances and their analogues. The case found that the criminal proceeds of the organized group, which amounted to approximately $2.1 million, were legalized by transferring the proceeds of drug sales to the bank accounts of controlled individuals, withdrawing them in cash and purchasing bitcoins that were transferred to anonymous electronic crypto accounts of the leaders of the criminal group, who disposed of them at their discretion.

Due to the impossibility of confiscation of the criminal income, the court on the basis of part 3 of article 48 of the CC, the sum of money equivalent to its size was collected from the convicted persons in solidarity (over $ 500 thousand from each of the convicted persons).

Case Study 8.12. Recovery of the value equivalent of the proceeds of crime

K. was found guilty by a court verdict for taking a bribe as an official in exchange for acts within his official authority for the benefit of the bribe-giver and was sentenced to a fine with life termination of his right to hold public office. Given that the subject of the bribe was not discovered during the pre-trial investigation, an equivalent sum of the bribe was recovered from the convicted person for the benefit of the state.

475. A value equivalent is also recovered from perpetrators if the property cannot be confiscated in accordance with statutory restrictions (property needed by the convict or his dependants - the convict's and his family's only housing, second-hand household items, utensils, clothing, etc.).

Case Study 8.13. Recovery of value equivalent if property cannot be confiscated

T. was convicted by a court for establishing and managing an organised criminal group, illegal

entrepreneurship and money laundering to eight years imprisonment. The case found that T. had set up an illegal business for the production and sale of alcoholic beverages, earning an especially large sum of money. T. legalized part of the criminal income by acquiring a land plot and the construction of a house on it. The court verdict confiscated this property to the benefit of the state.

However, in this case, it was clear that this house was the only housing of the convict and his family members and therefore was not subject to confiscation under the laws of the Republic of Kazakhstan. Under the protest of the GPO, the verdict was changed by the SC: the reference to confiscation of the land plot and the residential house was excluded, and the value of this real property in the amount equivalent to USD 40,000 was levied against T. to the state.

476. Restitution to the victims (compensation for criminal damages) is implemented through the institution of a civil claim in criminal proceedings, i.e., a property claim against the offender by the person who has suffered from the crime. Restitution to the victims takes precedence over confiscation because, under criminal law, confiscation applies to property that cannot be returned to the legal possessor.

477. Prosecutors are empowered to take civil actions for criminal damages caused to the state, as well as in certain other cases.

Case Study 8.14. Filing a claim by the prosecutor's office

In a criminal case against 3 individuals accused of committing illegal invoicing and ML, the prosecutor took a civil action for the recovery of criminal proceeds in the amount of KZT 55.2 million (approx. USD 170 thousand) to the state, which was considered by the court and satisfied in full.

478. The total amount of restitution to victims and compensation for damage caused to the state is significant. According to information from the compulsory execution agencies for 2017-2021, there were 113,384 enforcement documents in execution in the amount of 1,389.7 million US dollars on the recovery of damages in favour of individuals and legal entities caused by crimes, and 386,405 enforcement documents on the recovery of damages caused to the state in the amount of 3,520 million US dollars.

479. For information on confiscation for TF offence, see IO.9.

480. Enforcement of judicial decisions on confiscation of property and compensation for damages is the responsibility of the compulsory enforcement authorities. Bailiffs check the property situation of debtors. If property not seized during the pre-trial investigation is identified, such a decision is taken by a bailiff with the authorisation of the prosecutor and it is levied upon the court verdict.

Case Study 8.15. Identification of property of a convicted person during the execution of a sentence

D. was sentenced by a court for drug trafficking to 3 years and 6 months imprisonment. The case established that after the crime had been committed, the vehicle that had been used to transport drugs was sold by D. to a good-faith purchaser. This circumstance ruled out the confiscation of the vehicle by the State. In this regard, D. was ordered to pay the value of the vehicle (in an amount equivalent to $14,000) to the State.

During the execution of the sentence, the compulsory enforcement agencies established that the convicted offender had a flat and funds in his bank account. This property was seized and confiscated for the execution of the sentence in the part of the property charge.

481. Information about the work of compulsory enforcement agencies on the enforcement of court decisions on criminal cases in terms of confiscation of property and compensation for damages is provided in the table below.

Table 8.4. Enforcement of court decisions in criminal cases in terms of confiscation of property and compensation for damages

year	number of enforcement proceedings /amounting to (in USD)				completed enforcement proceedings / amounting to (in USD)				% of execution
	fines	confiscation	compensation for damages to natural and legal persons	compensation for damages to the state	fines	confiscation	compensation for damages to natural and legal persons	compensation for damages to the state	
2017	476.2 thnd.	394.7 mln	670 mln	473.9 тыс.	275.3 mln	531.6 mln	476.2 thnd.	394.7 mln	75,7
2018	831 thnd.	178.4 mln	1 971.5 mln	827 thnd.	66.5 mln	1 864.9 mln	831 thnd.	178.4 mln	89,4
2019	85.3 thnd.	192 mln	292.4 mln	53.5 thnd.	87.3 mln	154.5 mln	85.3 thnd.	192 mln	50,2
2020	5.9 mln	190.2 mln	250 mln	3.4 mln	73.3 mln	136.3 mln	5.9 mln	190.2 mln	47,8
2021	7 mln	434.4 mln	336.2 mln	2.7 mln	49.8 mln	183.3 mln	7 mln	434.4 mln	30,7
Total	14.4 mln	1 389.7 mln	3 520 mln	7.4 mln	552.2 mln	2 870.6 mln	14.4 mln	1 389.7 mln	69,5

482. The experts consider the downward trend in the execution of court decisions observed since 2019 as negative because the effectiveness of confiscation and compensation for damages (restitution to the victims) is ultimately determined by the actual execution of the court decision. In this regard, the work of compulsory enforcement agencies on the execution of court decisions on criminal cases of confiscation of property and compensation for property damage should be intensified.

483. There are no statistics on the enforcement of judicial decisions in criminal cases broken down by particular crimes.

484. Confiscated property goes into republican ownership (immovable property, unfinished construction projects, vehicles, ethyl alcohol and alcoholic products, tobacco and tobacco products, oil and petroleum products, securities, shares in authorized capitals, technical devices, precious metals, stones and products thereof) and municipal ownership (land, perennial plantings, animals, feedstuff, food products, grain, timber, medicines, mineral raw materials, minerals, agrochemicals and pesticides).

485. Further work with confiscated property received into state ownership is organized by the Committee of State Property and Privatization of the Ministry of Finance and its territorial subdivisions, and with property received into municipal ownership - by local executive authorities.

486. These authorities take the confiscated property from bailiffs and carry out its transportation to storage places, storage, valuation, sale through auctions or trade organizations or transfer to state legal entities or social service entities, destruction (in cases established by law), as well as its return in cases of revision of the court decision on confiscation.

Table 8.5. Information on property transferred to the state by the State Property and Privatization Committee (in millions of USD).

	2017	2018	2019	2020	2021	Total
Estimated value of property	15,7	21,9	22,9	5,6	5,1	71,2
Sold property in the amount of	9,9	14,5	15,7	4,9	4	49

487. The country has provided case studies of the transfer of confiscated property to state legal entities (including prosecution authorities) and social service entities. According to experts, this method of disposal of confiscated property is an effective management mechanism.

Case Study 8.16. Management of confiscated property

An interagency operational investigative group of the NSC and officers of other LEAs investigated a criminal case against members of a transnational criminal association composed of 24 individuals, including law enforcement and procuracy officials. The leader of the criminal community, T., and other participants were accused of committing a number of crimes (murder, robbery, brigandism, illegal arms trafficking, establishment and direction of a transnational criminal association, tax evasion, bribery, etc.).

Disposing of the proceeds derived from criminal activity, the criminal community members purchased 8 land plots, 12 cottages, 40 cars, over 180 jewelry items and precious stones, 99,9% of shares in the authorized capital of the group of companies which consisted of large industrial enterprises and social facilities, as well as other property. The above property was seized as part of a pre-trial investigation.

The court sentenced T. for the totality of the crimes committed to imprisonment for a term of 21 years with confiscation of property obtained by criminal means or acquired with criminally obtained funds, with life-long deprivation of the right to hold certain positions. Other members of the criminal association were sentenced to various terms of imprisonment with confiscation of property.

During the execution of the sentence in terms of confiscation of property, shares in the authorized capital of the group of companies were transferred to the state, a social facility (palace of culture), 8 land plots and 4 cottages were transferred to the executive authority of Shymkent City. Vehicles were put on the electronic trading platform for further transfer to state legal entities.

Case Study 8.17. Management of confiscated property

The court sentenced 36 members of organized criminal associations and criminal groups for corruption-related offences (taking bribes in especially large amounts, abuse of power), money laundering and other offences to imprisonment for a term of 3 to 16 years with confiscation of criminal property. In the course of the pre-trial investigation, the interagency operational investigative group of the GPO and ACA found that the members of the organized criminal group, which included financial police officers, prosecutors, tax officials and bank clerks, established 86 fake companies with the criminal proceeds amounting to KZT 77 billion (over USD 230 million) legalized by introducing it into the legal circulation. Besides that, the criminally obtained funds were used to purchase vehicles and other property, which were seized during the pre-trial investigation.

During the execution of the sentence in terms of confiscation of property, 2 helicopters and 5 cars were transferred to the territorial divisions of the internal affairs bodies, Anti-Corruption Service and State Revenue Committee of the MoF.

488. It should be noted that the above agency does not keep separate records on the assessment and sale of property confiscated under criminal and administrative cases or on other grounds; therefore, these indicators cannot be compared with the statistical data of the compulsory enforcement agencies.

489. Thus, the country has demonstrated a successful practice of confiscation of proceeds of crime, property acquired with criminally obtained funds, including fictitiously held by third parties, instrumentalities and means of committing crimes and the cash equivalent of the proceeds of crime. The rights and interests of bona fide third parties are effectively protected. Measures have been taken to recover criminal assets transferred to foreign jurisdictions. The practical application of pretrial confiscation safeguards the interests of the State and victims by ensuring that property is returned to the State in a timely manner or to compensate for damage caused by a crime.

490. Further improvements in the effectiveness of confiscation will be facilitated by increased efforts by competent authorities to adopt provisional measures and give effective effect to confiscation judgements and restitution awards.

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

491. Customs authorities are not LEA per se, do not belong to the bodies engaged in the CIDA and pre-trial investigative authorities. However, they carry out activities aimed at detecting, preventing and suppressing criminal and administrative offences in the field of customs legislation.

Table 8.6. Information on the total number of passenger customs declarations (PCDs) submitted and the volume of cash declarations.

Year	Entering		Departure		Total	
	Number of PCDs	**Amount, equivalent mln USD**	**Number of PCDs**	**Amount, equivalent mln USD**	**Number of PCDs**	**Amount, equivalent mln USD**
2017	140	10.9	3 571	109.1	3 711	120
2018	215	39.6	4 079	134.3	4 294	173.9
2019	272	100.4	3 919	146.3	4 191	246.7
2020	73	11.8	1 546	58.8	1 619	70.6
2021	313	11.1	4 892	200.9	5 205	212
Total	1 013	173.8	18 007	649.4	19020	823.2

492. Between 2017 and 2021, the customs authorities detected 577 administrative offences related to non-declaration (false declaration) of cash. A significant decline in the detection of such offences in 2020 is due to a sharp decrease in passenger traffic associated with the anti-COVID measures during the pandemic.

Table 8.7. Number of detected administrative offences related to non-declaration (false declaration) of cash

Year	**Number of detected administrative offences**	**Fines amounts, USD**	**Total amount of undeclared money, USD**
2017	129	24 506.6	1 339 973
2018	106	7 395.7	1 275 114
2019	145	9 697.6	1 855 362.6
2020	36	2 303.8	1 669 547
2021	163	11 058.5	5 298 678.4
Total	759	54 962.2	11 438 675

493. In general, the number of detected offences is insignificant. According to the experts, this is due to a number of factors, the main one being the absence of customs control within the EEU. Besides that, customs authorities do not have direct access to the LEAs/SSAs information systems and can obtain the required information from the competent authorities only on request or proactively.

494. Representatives of customs authorities explained that the application of enhanced customs control measures is based on the information provided by LEAs/SSAs or on the profiling system. However, this system is not automated and the effectiveness of its application largely depends on the human factor.

495. The lack of access to information about the criminal record of individuals and other information about involvement in ML/TF makes it very difficult for customs authorities to make a prompt decision on the application of enhanced customs control measures based on the risk-based approach (for example, when obtaining a list of passengers on an air flight as part of preliminary informing).

496. Non-declaration (false declaration) of cash, which entails administrative liability, was detected by the customs authorities when importing (exporting) currency from the UAE, Turkey, Korea, Ukraine, Georgia, Uzbekistan, Germany, and China.

Table 8.8. Statistics of seized cash that was the subject of administrative offences.

Currency type	**2017**	**2018**	**2019**	**2020**	**2021**	**total**
US dollars	1 339 973	1 275 114	1 723 434	1 669 547	4 211 588	10 219 656
Euros	-	-	25 275	-	589 120	614 395
Russian rubles	-	-	-	-	28 692 300	

497. At the same time, confiscation of the subject of an administrative offence is not applied. This is due to the fact that under applicable law confiscation is applied only by the court, while the proceedings on administrative offences under CAO Article 551(3) (non-declaration or false declaration) are carried out by the customs authorities. CAO Article 551(3) does not contain confiscation. Illegally transported funds, which are the subject of an administrative offence, are returned to the offender.

498. Another negative factor is the insignificant amount of fines for this administrative offence. When it

was discovered that over 11.4 million US dollars in cash had not been declared, the individuals responsible were sanctioned for only 54,900 US dollars.

499. There were no facts on the detection of undeclared cash currency in international postal items in the assessed period.

500. When a criminal offence is detected by the customs authorities, the materials are submitted to the EIS, whose purview includes pre-trial investigation into this category of criminal cases.

501. The detection of such facts was sporadic: 2 in 2017, 2 in 2018, 1 in 2020, and 3 in 2021. At the same time, the total amount of seized money, which was the subject of a criminal offence, in this period was also insignificant (USD 273,400, EUR 73,535, KZT 247,000).

502. The EIS in this period conducted pre-trial investigations into 8 cases provided by CC Article 234, in which the courts pronounced guilty sentences with confiscation of the subject of economic smuggling.

Case Study 8.18. Conviction for cash smuggling

In March 2021, the customs officers together with the EIS revealed the fact of non-declaration of foreign cash (USD, EUR, KZT) in the total amount of USD 99,100 by Kazakh national A., who arrived on flight "Antalya-Almaty". A. was sentenced by the court under CC Article 234(1) to a fine in the amount equivalent to USD 274. The subject of smuggling (dollars, euros and KZT) was confiscated into the revenue of the state.

503. Taking into account the small number of detected offences related to non-declaration (false declaration) of cash, non-application of confiscation in administrative proceedings and isolated facts of convicting persons for economic smuggling with confiscation of property, the experts conclude that confiscation of such funds is not effective, proportionate and dissuasive and does not help to suppress the cash couriers' activities.

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

504. The activities of the competent authorities are aimed at ensuring the implementation of the state policy in terms of confiscation of criminal assets, identification and return of criminal assets from foreign jurisdictions, and criminal injuries compensation.

505. The country provided case studies of confiscation of criminal property in criminal cases involving offences that, according to the NRA, are classified as high-risk ML offences (tax and corruption crimes, economic crimes, theft by misappropriation and fraud, as well as illicit drug trafficking).

506. However, there is no information on the total number of convictions for which confiscation was applied with a breakdown by predicate offence.

507. The agencies' approaches to statistical recording of provisional measures related to confiscation, enforcement of confiscation sentences and sale of confiscated property vary. The statistical and analytical records provided are fragmented and incomparable. There are no centralized records that would allow to analyze the application of confiscation from the moment a criminal property is identified to its transfer to the state.

508. In view of the above, it was not possible to draw definitive conclusions about the consistency (inconsistency) of confiscation to ML/TF risk assessment.

Overall conclusion on IO.8.

509. Confiscation of property obtained by criminal means or acquired with criminally obtained funds and instrumentalities of crime, compensation for property damage caused by crimes is a priority task and means of implementation of the state criminal policy in the anti-crime sphere.

510. Confiscation is carried out as part of the criminal prosecution of a person and is a direct consequence of the commission of a crime. Confiscation of incomes, the legitimacy of which has not been confirmed,

does not take place.

511. The pre-trial investigative authorities are exercising the powers granted to them for fulfilling their procedural duties to secure confiscation. Measures have been taken to intensify their efforts to search for assets abroad and their return. However, statistical indicators reflecting the results of these activities indicate the need to improve their effectiveness.

512. Aspects hampering the application of confiscation include the lack of other practical mechanisms for confiscation of VAs other than the voluntary granting of access to such assets by the perpetrator.

513. The courts apply confiscation of the proceeds of crime, property acquired with criminal funds, instrumentalities and instrumentalities of crime, and property of equivalent value.

514. The work on the execution of court decisions in terms of confiscation of property and compensation for criminal damage should be improved and intensified.

515. Confiscation of non-declared (falsely declared) cash in administrative proceedings is not applied at all, and in criminal proceedings it is sporadic. In this regard, the disruption of cash couriers' activities through the application of confiscation is not effective.

516. The country has provided statistical and analytical information on the use of confiscation. However, due to their incomparability and the deficiencies in statistical record-keeping noted in the text, it was not possible to reach definitive conclusions on the consistency of confiscation with the NRA findings.

517. **Kazakhstan is rated as having a moderate level of effectiveness for IO.8.**

CHAPTER 4. FINANCING OF TERRORISM AND PROLIFERATION FINANCING

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. The country's authorities clearly understand the threat of international terrorism and the external and internal factors that contribute to the involvement of citizens in terrorist activities, among which the most relevant for Kazakhstan is the radicalization of the population through involvement in destructive religious movements and the propaganda of terrorist ideas.

2. Countering terrorism and religious extremism is a state policy priority integrated into national policy documents and implemented in a systematic and comprehensive manner both within the country and through cooperation with international partners.

3. The country has taken measures to coordinate the actions of all actors engaged in the fight against terrorism and to ensure a high level of interaction among all government authorities and organizations.

4. TF detection and prosecution is one of the activities of LEAs/SSAs in the field of counter-terrorism. Operational capabilities of the FIU are actively used for the purposes of detecting TF, and parallel financial investigations are conducted. National security agencies ensure the proper quality of the CIDA and pre-trial investigations into TF crimes. At the same time, taking into account that combating terrorist offences is also within the purview of the EIS and MIA, the efforts on detecting TF by these LEAs should be intensified.

5. LEAs and SSAs have the necessary human, material and technical and information and analytical resources. Considerable attention is paid to training and professional development of the staff in the field of combating terrorism and its financing, and the necessary training and methodological base is available.

6. TF is prosecuted for a variety of activities, including raising, movement and use of funds, providing informational and other services to terrorists. At the same time, TF offences were often detected after the transfer of funds rather than at the stage of TF-related fundraising, so there were no instances of TF funds being identified and seized.

7. The results of the prosecutions are consistent with the NRA findings and the country's risk profile. The entry into force of a conviction entails the designation of the person convicted of TF in the National List of persons involved in the financing of terrorist activities.

8. Guilty persons are convicted, and the sanctions applied by courts to natural persons for TF offences are effective, perform the function of private and general prevention, i.e. have a dissuasive nature and are generally proportionate, since they are imposed taking into account the public danger of the act and personal background. A total of 34 people were convicted of TF offences in 2017-2021, and 10 more were convicted in the first half of 2022. There were no cases of acquittals or termination of proceedings by the courts based on exonerating grounds.

9. The information provided did not allow to draw a definitive conclusion about the nature of sanctions against legal persons.

10. In cases where it is impossible to secure a conviction for TF, prosecution for other offences (if any) is applied. In order to suppress the facts of involvement of citizens in terrorist offences, including TF, a set of preventive measures is implemented.

Immediate Outcome 10

1. In general, Kazakhstan has built and uses a system that meets the requirements for the application of targeted financial sanctions without delay. Despite the introduction of amendments to the regulatory

legal framework of the Kazakhstan in 2020 aimed at stipulating at the legislative level the mechanisms and procedures for the implementation of the TFS requirements by the obliged entities and individual government authorities, Kazakhstan has demonstrated that, before the adoption of these amendments, TFS in accordance with the UN sanction lists were also applied without delay. Besides that, Kazakhstan has demonstrated its ability to apply TFS in accordance with national lists, as well as to take action to freeze assets in response to requests from third countries pursuant to UNSCR 1373.

2. Kazakhstan, on average, publishes lists on its official website and disseminates them to FIs, DNFBPs and VASPs within a few hours. In practice, in most cases, the publication of lists (additions, amendments or removals) takes no more than 30 minutes. The publication of the lists is the legal basis for the obliged entities to apply measures for freezing funds and other assets of persons within no more than 24 hours.

3. Kazakhstan has an effective mechanism for suspending transactions administratively for 16 days, (i.e., an administrative freeze for 15+1 days) when there is suspicion that the transaction relates to ML/TF.

4. As part of the formation of the national sanction list, terrorist and extremist activities are considered as grounds for designation. In the assessed period, more than 2,800 individuals and entities within the country were designated in the sanction lists. Kazakhstan has sent two requests to third countries (within the EAG region) regarding 159 persons pursuant to UNSCR 1373. At the same time Kazakhstan has sent the above requests only to the EAG member states. Kazakhstan has not sent any requests for designation of individuals or entities in international UN sanction lists.

5. The Kazakhstan carries out certain work to control NPOs in order to prevent them from being misused for TF purposes without prejudice to their legitimate activities. The country provides for measures aimed at preventing registration of NPOs exposed to such risk, termination of their activities and liquidation, as well as applying sanctions for non-compliance of NPOs with the relevant control requirements of the country. At the same time, the work is generally based on the NRA and TF SRA findings in terms of the misuse of NPOs, according to which the average risk level is assigned to charitable and religious organizations.

6. Interagency cooperation between supervisory and law enforcement authorities has been built in the country, which generally allows, if necessary, to collect and verify information about the activities of NPOs and their possible involvement in TF in a timely manner, as well as to exchange it, including at the international level. At the same time, no cases of involvement of NPOs in TF-related activities were identified in the assessed period.

7. The main focus of the competent authorities in their work with NPOs is to ensure transparency of transactions with funds and other assets, raising and accounting of funds and incoming donations, including from abroad, which generally corresponds to the profile of the identified risk. However, there is no proper control over the purposeful use of the provided financial assistance.

8. NPOs sufficiently understand the vulnerability of organizations to the use for TF purposes, but do not fully have the mechanisms of their own actions in the event of such situations.

9. The supervisory authorities for NPOs apply measures of control (monitoring) over the activities of NPOs, but such measures are more of a unified approach to the supervision and monitoring over NPOs, although comply with the risk-based approach.

10. Kazakhstan seeks to deprive terrorists, terrorist organizations and terrorist financiers of their assets and instrumentalities of crime by various methods, including designation, freezing of funds and confiscation as part of TF investigations and proceedings.

11. The measures taken by the authorities of the Kazakhstan are generally consistent with the overall TF risk profile of the country.

Immediate Outcome 11

1. Kazakhstan has a unified legal framework in the field of combating PF and TF. In general, the country has built and uses a system that meets the requirements for the implementation of targeted financial sanctions without delay.

2. The FMA is the competent authority responsible for the formation and maintenance of the list of individuals and entities involved in PF. The FMA also plays an important role in informing FIs, DNFBPs, VASPs and individual government authorities about the obligations to apply TFS and raising awareness in the private sector.

3. No funds or other assets owned by individuals or entities designated in the PF list were identified in the Kazakhstan in the assessed period. The requirements for application of PF-related TFS also apply to virtual assets. VASPs registered in the AIFC and not registered in the AIFC are required to comply with all AML/CFT/CPF legal requirements. At the time of the on-site mission, Kazakhstan has not implemented the freezing of virtual assets on PF-related grounds.

4. FIs and DNFBPs may have difficulties effectively implementing PF-related TFS due to deficiencies in identifying the BO of the customer or party to the transaction. At the same time, the obliged entities also use automated systems and commercial databases to most effectively implement their TFS-related obligation when conducting identification. The FMA and other supervisors also clarify FIs' and DNFBPs' obligations to apply TFS.

5. The obligation to apply PF-related TFS does not apply to all natural and legal persons, but only to FIs, DNFBPs and VASPs, because there are no provisions in the legislation of the Kazakhstan that directly stipulate liability for violation by all natural and legal persons of the ban on providing funds and other assets to persons designated in the PF-related list.

Recommended Actions

Immediate Outcome 9

1. The authorities need to continue to implement the national counter-terrorism strategy, focusing on identifying and suppressing TF, including the financing of terrorist activities within the country.

2. The activity of LEAs responsible for combating terrorist offences (MIA, EIS) should be intensified in detecting and suppressing TF offences.

3. Prosecution authorities should take additional organizational and practical measures to detect TF offences at the stage of fundraising and seize funds intended for TF purposes.

4. The competent authorities should ensure the maintenance of disaggregated statistical records of terrorist offences and TF offences under the Criminal Code articles, which provide for liability for both terrorist and extremist acts.

5. It is necessary to review the approaches to liability of legal persons, establish the possibility of applying a range of proportionate and dissuasive sanctions, mechanisms for the effective application of sanctions to legal persons for TF.

Immediate Outcome 10

1. Kazakhstan should expand the geography of requests for asset freezing under UNSCR 1373 beyond the Eurasian region.

2. The Kazakhstan should continue the practice of identifying individuals with a view to filing proposals for their designation in the relevant sanction lists of the UNSC Committees. For this purpose it is necessary to analyze the existing national sections of the lists for the presence of persons falling under the designation criteria.

3. The government authorities should continue raising awareness among FIs, DNFBPs and VASPs regarding their obligations to implement TF-related TFS, including through workshops, development of practice guidelines and typologies.

4. The country's competent authorities should improve their supervision over NPOs and application of control (monitoring) measures to NPOs in accordance with the risk-based approach.

5. Consider developing additional targeted measures in relation to NPOs vulnerable to the use for TF purposes, including in terms of ensuring control over the spending of funds by charitable and religious organizations, based on certain threats and risks of using NPOs for TF purposes.

6. Ensure regular updating of the sectoral risk assessment of NPOs and use all possible sources to identify the types of NPOs that are at risk of involvement in TF.

7. Consider the possibility of providing NPOs with up-to-date information on the TF/PF List and receiving timely notifications about its updates.

Immediate Outcome 11

1. Take effective measures, including legislative changes, to ensure that the mandatory freezing requirements within the frame of TFS apply to all natural and legal persons (not only FIs, DNFBPs and VASPs) and that all natural and legal persons are prohibited from directly or indirectly making any funds, financial assets or economic resources available for use by individuals or entities designated in the UN lists.

2. Consider mechanisms of strengthening the ability of the obliged entities to identify companies owned or controlled by designated persons in order to identify possible cases of avoiding to comply with PF requirements.

3. Continue to raise and ensure awareness of FIs, DNFBPs and VASPs, including by developing detailed guidance for the obliged entities on the practical application of PF-related TFS.

518. The relevant Immediate Outcomes considered and assessed in this section are Immediate Outcomes 9-11. Recommendations 5-8 (as well as 1, 2, 30-32, 37, 39, 40) are used in assessing effectiveness).

4.2. Immediate Outcome 9 (TF investigation and prosecution)

4.2.1. Prosecutions/conviction of types of TF activity consistent with the country's risk profile

519. According to the 2018 NRA conclusions, the TF threat level was defined as high. The country has taken a set of measures aimed at ensuring the security of individuals, society and the state from violent manifestations of terrorism and religious extremism, detecting and suppressing terrorist acts at the stage of their preparation, reducing the influence of external factors on the radicalization of the population and the number of people who share extremist ideas.

520. In the period since the aforementioned risk assessment was conducted in Kazakhstan, thanks to the consolidated counter-terrorism efforts of the authorities, there have been significant changes in the crime rate.

521. No terrorist acts were committed in the country in 2017-2021, while 11 such offences were committed in Kazakhstan in the period 2011-2016, which resulted, *inter alia*, in the deaths of people. The number of terrorist acts suppressed at the stage of preparation was 20, which is significantly lower than the number of such facts detected in the previous period (96).

522. There was a steady decline in the number of other terrorist manifestations. In particular, the number of offences under CC Article 257 (establishment, direction and participation in a terrorist group) decreased from 40 in 2017 down to 5 in 2021; under CC Article 256 (propaganda of terrorism or public calls to commit an act of terrorism) - from 133 down to 61; under CC Article 259 (recruitment, training or arming persons

to organize terrorist or extremist activities) - from 13 down to 5; under CC Article 258 (financing of terrorist or extremist activities and other aiding in terrorism or extremism) - from 18 down to 7 [21].

Table 9.1. Number of some terrorist and extremist offences broken down by CC article

RK CC article	2017	2018	2019	2020	2021	total
256 (terrorist propaganda or public calls to commit an act of terrorism)	133	82	66	49	61	**391**
257 (establishment, direction and participation in a terrorist group)	40	17	35	9	5	**106**
258 (financing of terrorist or extremist activities and other aiding in terrorism or extremism)	18	14	3	9	7	**51**
259 (recruitment, training or arming of persons for the purpose of organizing terrorist or extremist activities)	13	11	2	7	5	**38**

523. The number of adherents of destructive religious movements[22] decreased (from 309 down to 147) due to the measures taken to prevent illegal activities of persons classified according to the 2018 NRA findings as persons with a high degree of threat of committing TF. Since 2018, there have been no cases of Kazakh nationals traveling to areas of terrorist activity to participate in terrorist activities. According to the information available to the competent authorities, the number of citizens of Kazakhstan that are participants of international terrorist organizations (hereinafter the ITO) has decreased by half (from 80 down to 40). The number of Kazakh nationals traveling independently to receive theological education has reduced (from 360 down to 78).

524. Due to this positive trend, the TF risk level was rated in the 2021 NRA as medium.

525. According to the 2021 NRA findings, the national authorities clearly understand the threat of international terrorism, external and internal factors contributing to the involvement of citizens in terrorist activities, among which the most relevant for Kazakhstan is the radicalization of the population through involvement in destructive religious movements and the propaganda of terrorist ideas.

526. According to the NRA findings, the main threat of terrorist financing is still posed by adherents of non-traditional (destructive) movements, Kazakh nationals who travel to areas of high terrorist activity to participate in the ITO activities, as well as individuals returning from such areas, participants of terrorist organizations, illegal armed groups and radical groups located outside the territory of Kazakhstan and involving Kazakh nationals in terrorist activities through the Internet, as well as Kazakh nationals traveling independently to foreign jurisdictions to receive theological education.

527. Thus, the 2021 NRA conclusions regarding the assessment of categories of persons with a high probability of committing TF offences have not actually changed. Persons serving prison sentences for terrorist offences were excluded from this category. As representatives of the competent authorities explained, this is due to the fact that by virtue of comprehensive and systematic work aimed at deradicalization of these convicts, prevention of illegal manifestations on their part, including propaganda of destructive ideas among other convicts, re-socialization and preventive measures, no facts of repeated terrorist manifestations were registered after their release.

528. The TF sources were most often money from legal sources (own funds, including proceeds of the property sale).

529. The main TF typologies include money transfers through international transfer systems or to card accounts for the ITO members followed by their cashing out in the territories of states bordering the ITO war zones (Syria, Pakistan, Afghanistan). The TF typologies provided by the competent authorities indicate that almost all of the identified facts were of an external nature, that is, related to the transfer of funds, provision of other services of a financial and informational nature to the ITO members engaged in illegal

[21] Centralized statistical records of offences under CC Articles 258, 259 and other CC articles establishing liability for both terrorist and extremist acts are not kept separately by type of activity (terrorist or extremist.

[22] Destructive religious movements (organisations) - structures spreading radical religious ideas, inciting inter-religious and international conflicts, denying state institutions (laws, authorities), traditional family values, encouraging to renounce civil duty (getting education, serving in the army, etc.). These include, in particular, ITOs such as al-Qaida, the Taliban, ISIL and others.

activities outside the Kazakhstan borders. At the same time, according to the NSC, the goals of funding have changed. If previously TF was carried out directly to support terrorist activity (purchase of weapons, ammunition, preparation of terrorist acts), now the vector has shifted to the support of the ITO members or providing them with funds to return to Kazakhstan.

530. In the assessed period, no facts of financing terrorist acts suppressed on the territory of Kazakhstan, activities of terrorist organizations and other terrorist offences were revealed. As explained by representatives of the competent authorities, these unlawful actions were carried out through self-financing. At the same time, the threat of financing terrorist activities within the country is not excluded, which is taken into account by the competent authorities in their activities.

531. A total of 34 persons were convicted of TF offences in 2017-2021, and 10 more persons were convicted in the first half of 2022. There were no cases of acquittals or termination of proceedings by courts on exonerating grounds (see Table 9.2).

532. The results of prosecutions and convictions (listed below in the analysis) are generally consistent with the NRA findings and the country's risk profile.

4.2.2. TF identification and investigation

533. In the Kazakhstan, activities aimed at detecting, suppressing and uncovering TF offences, as well as ML offences, are carried out in the form of CIDA and pre-trial investigations.

534. In the course of the CIDA, the collection and processing of information in order to establish the fact of preparation or commission of an offence takes place. The basis for initiating the CIDA is any information about indicators of illegal activities, which is verified through the implementation of a set of the police intelligence operations. When during the CIDA indicators of an offence are detected, the information is recorded in the URPI and submitted to the investigative units for pre-trial investigations.

535. As part of the pre-trial investigation, investigative and other procedural actions are used to prove the fact of the offence, the circumstances of its commission and the guilt of the offender.

536. TF offences may be detected during the pre-trial investigation into other offences. In this case, a TF offence is registered in the URPI and a pre-trial investigation is conducted into it (in separate proceedings or in proceedings combined with a previously detected offence).

537. Given the division of powers of prosecution authorities established by the Kazakh legislation, the main authority responsible for detecting, suppressing and investigating terrorist offences, including TF, is the NSC. The MIA is more responsible for combating extremism. The EIS is responsible for detecting and suppressing the illegal movement of weapons, ammunition and other items that can be used as means of committing terrorist offences across the EEU customs border, as well as preventing, detecting and suppressing sources, channels and methods of terrorist financing.

538. A special operational unit, the Department for Combating International Terrorism, was established within the NSC, whose independent activity includes detecting and countering TF. The Investigative Department of the NSC specializes investigators in conducting parallel financial investigations and pre-trial investigations of TF cases.

539. Similar approaches are taken in the MIA, which has established the Department for Countering Extremism and Terrorism (an operational unit) and the Investigative Department.

540. In addition to the operational and investigative departments, the EIS has also established an independent unit whose staff is responsible exclusively for conducting parallel financial investigations.

541. The General Prosecutor's Office has a service of special prosecutors, whose purview includes conducting pre-trial investigations. As explained by the GPO representatives during the on-site mission, criminal cases of TF offences were not investigated by prosecutors. Besides that, prosecutors supervise the legality of the CIDA and pre-trial investigations by authorizing the police intelligence operations, coordinating investigative actions and giving instructions in criminal cases.

542. For pre-trial investigations into complex, multi-count criminal cases, operational investigative groups (departmental and interagency) are established).

543. Upon completion of the pre-trial investigation, the prosecution authority forwards the criminal case to the procurator for referral to a court. If any deficiencies or incompleteness of the pre-trial investigation are found, prosecutors have the right to return the case to the prosecution authority for further investigation, but in TF-related cases there were no such facts.

544. After a criminal case is referred to the court for consideration on the merits, criminal prosecution is carried out by prosecutors, who represent the state in a prosecution. As explained by representatives of the agency, there is no specialization of public prosecutors in TF-related cases, but according to established practice, the representation of the state in a prosecution in this category of criminal cases is assigned to the most qualified officers.

545. Public prosecutors are obliged to withdraw charges when circumstances excluding criminal prosecution of a person (lack of evidence, failure to prove guilt, etc.) are established. The withdrawal of charges by the public prosecutor leads to the termination of criminal prosecution. There were no such facts in TF-related cases.

546. The final procedural decision in a case is taken by a court (whether it issues a guilty verdict or an acquittal, or an order to terminate proceedings in the case).

547. Of the total number of criminal cases registered under CC Article 258, the financing of terrorist activities or other aiding in terrorist activities accounted for 72.5% (37 cases):13 in 2017, 9 in 2018, 1 in 2019, 8 in 2020, 6 in 2021. At the same time, the NSC detected 29 crimes of TF, and 8 crimes of EIS (the cases were subsequently transferred to the NSC for pre-trial investigation, as the perpetrators committed other crimes in addition to TF which fall under the exclusive jurisdiction of the NSC). Other crimes registered in the URPI, under CC Article 258 were related to the financing of extremist activities.

548. Information on specific methods and techniques for detecting terrorist offences, including TF, is classified due to the specificities of the national security agencies' activities. During the on-site mission, the NSC representatives explained that the full range of the police intelligence operations and investigative actions are used to detect TF offences, including parallel financial investigations, and provided specific case studies.

Case Study 9.1 (identifying TF indicators using the FIU information)

The NSC received operational information that Kazakh national K. was in contact with an unidentified fighter of ITO "DAISH" via the "Telegram" messenger. At this individual's direction, K. purchased three SIM cards and transmitted the activation codes for T.'s numbers to a member of ITO "DAISH" in Syria. In cooperation with the FIU, financial transactions of K. were checked and it was found that he had transferred money to T. through the international money transfer system in the amount of USD 150. A pre-trial investigation was initiated against K. under CC Article 258(1). The court found him guilty of financing terrorist activities and sentenced him to imprisonment for a term of 5 years.

549. There was a fact of revealing the financing of the travel of a Kazakh national to a war zone for his subsequent participation in terrorist activities.

Case Study 9.2 (identifying the financing of the travel of a Kazakh national to a war zone)

As part of a pre-trial investigation against Kazakh national A., it was established that in 2015 he went to Syria with the purpose of receiving terrorist training and subsequent participation in the armed jihad of ITO "DAISH". While in Syria, A. recruited and persuaded Kazakh nationals, including T., to go to Syria. During a parallel financial investigation in cooperation with the FIU, it was found that in order to finance T.'s travel to Syria for participation in the ITO terrorist activities, A. transferred money in the amount of USD 300 via the money transfer system, which the latter cashed and used to prepare the travel, but his intention was not completed due to the suppression of his actions by the NSC. Based on these facts, a

pre-trial investigation was initiated against A. under CC Articles 258 (TF) and 259 (recruitment for the organization of terrorist activity). The proceedings were suspended, and A. was put on the international wanted list.

In May 2019, as part of the "Jusan" special operation (an operation to repatriate Kazakh citizens from areas of terrorist activity), A. was taken to the territory of Kazakhstan.

The court found him guilty of participating in the activities of a terrorist organization, undergoing terrorist training, recruiting and financing terrorist activities and sentenced him to imprisonment for a term of 13 years.

550. From a positive perspective, it should be noted that the competent authorities conduct parallel financial investigations in all cases when persons with a high TF risk assigned to them commit offences that generate criminal proceeds. In particular, according to the MIA information for 2017 - 6 months of 2022, adherents of destructive religious movements committed 2,133 non-terrorist offences (theft, fraud, extortion and robbery). For each offence, parallel financial investigations were conducted to identify the possible intent to use the criminally obtained funds for TF purposes, but there were no such facts.

551. LEAs/SSAs have access to a wide range of information, including financial intelligence, for the purpose of conducting parallel financial investigations. The Information System of LEAs/SSAs (Law Enforcement and Special Authorities Information Exchange System) is integrated with 81 databanks of 26 authorized bodies and government authoritiies, 21 STBs (for more details, see IO.7).

552. One of the areas of parallel financial investigations is the identification and seizure of criminal assets and instrumentalities of crime and their seizure for the purpose of subsequent confiscation. In TF cases, instrumentalities of crime (cell phones, weapons) were the most frequently identified. The facts of seizure of money were isolated. This is due to the fact that, as a rule, the offenders used funds from legal sources for TF purposes. The amount of one transaction ranged from USD 150 to 2 thousand, and the total amount of funds transferred for TF purposes in all criminal cases was USD 29 thousand and KZT 12.5 million. The insignificant amount of funds used for TF indicates the low level of well-being of the offenders. Besides that, TF offences were detected after the transfer of funds and not at the stage of fundraising for TF, therefore there were no facts of identification and seizure of funds intended for TF purposes.

553. If necessary, the operational capabilities of the FIU are used for the purpose of identifying TF indicators. The level of cooperation with the FIU in the prosecution of terrorism and TF offences is high. Between 2017 and 6 months of 2022, the NSC received 250 proactive materials from the FMA, 193 of which were TF-related. The NSC sent 41 requests to the FMA, including 3 TF-related requests. The NSC representatives noted that the FMA information was used in 110 police intelligence operations, of which 78 were TF-related, as well as in the pre-trial investigations into 96 criminal cases, of which 30 were TF offences. Case studies were provided where the FMA proactive information was the basis for initiating pre-trial investigations into TF cases.

Case Study 9.3 (TF investigation based on the FIU's proactive information)

The NSC received information from the FIU about suspicious transactions - the transfer of funds via STBs to the accounts of persons located in countries bordering the zone of terrorist activity. During the processing of this information, they identified Kazakh national Sh., an adherent of destructive religious movements, sharing and supporting the idea of armed jihad, who repeatedly transferred funds to bank accounts of persons taking part in the ITO activities against the Syrian government forces.

During the police intelligence activities and pre-trial investigation, in addition to TF indicators, Sh. was proven guilty of terrorism propaganda, incitement to religious hatred and illicit drug trafficking. The court sentenced Sh. for the totality of the crimes committed to imprisonment for a term of 7 years and 6 months.

554. The procedural obligation of the prosecution authorities is a comprehensive, complete and objective

investigation of all the case circumstances, including the establishment of the role of an individual and the degree of involvement in the offence, the mechanism (method) of its commission, the causes and conditions contributing to the commission of the offence.

555. Cases of involvement of individuals in TF, as well as cases of committing an offence through the use of individuals unaware of the criminal nature of the actions being committed, have been detected.

Case Study 9.4 (TF with the use of uninformed persons)

During the correspondence in the "VKontakte" social network, a participant of ITO "DAISH" asked Kazakh national T. for financial assistance and provided payment details. T. entered into a criminal conspiracy with Sh. and deposited KZT 104.9 thousand (approx. USD 300) into the bank account of the latter via a payment terminal. Sh. cashed the money by withdrawing it from the card. In order to realize his intent to finance terrorism, Sh. found citizen D., who, being unaware of the offence being committed, transferred money through the money transfer system to Turkey using the details provided by Sh.

The court found T. guilty of financing terrorist activities by prior conspiracy of a group of persons and sentenced him under CC Article 258(2) to imprisonment for a term of 6 years. The case against Sh. was singled out for considering in a separate procedure.

556. When persons who conduct financial transactions are aware that the funds are intended for those involved in terrorist activities or terrorist organizations, they are criminally liable for TF.

Case Study 9.5 (TF with the use of informed persons)

As a result of monitoring social networks it was found that Kazakh national I. published in the public domain materials aimed at inciting religious hatred and discord and terrorist propaganda. As part of a parallel financial investigation of the NSC using the FIU operational capacity, it was found that I. transferred USD 300 in her own name by bank transfer to a Tajik native Yu. involved in terrorist activities, who, in turn, was to transfer the money to M., taking part in the activities of ITO "DAISH" in the territory of Syria. I. transferred the money at the request of M.'s parents and she was aware that M. was a member of the ITO. The court sentenced I. for the totality of the crimes committed, including TF, to imprisonment for a term of 6 years.

557. It should be noted that in addition to raising and provision of money and other property, TF offences (CC Article 258) in Kazakhstan also include the provision of information and other types of services for terrorist activities. Case studies of the identification and prosecution of these types of illegal activities are provided.

Case Study 9.6 (TF through the provision of information and other services)

1. In the course of the police intelligence operations, Kazakh national K. was identified, who, in the "Telegram" messenger, using accounts from various numbers of mobile operators, corresponded with a member of ITO "DAISH". Being aware of his intention to carry out terrorist acts in Almaty, K. provided the terrorist with information about the location of executive and law enforcement authorities in the city. The court found K. guilty and sentenced under CC Article 258(1) to imprisonment for a term of 5 years.

2. Kazakh national S. for a financial reward agreed to assist five individuals who intended to travel to Syria through Turkey to participate in the ITO terrorist activities. For this purpose S. flew to Istanbul, where he acted as an intermediary between these individuals and the person who carried out their illegal transfer to Syria. The court found S. guilty of providing information and other services to persons involved in terrorist activities and sentenced him under CC Article 258 to imprisonment for a term of 5 years.

3. Kazakh national N., an adherent of a destructive radical movement, entered into correspondence via "Telegram" messenger with ITO member L., who was taking part in combat operations in Syria. L. sent N. instructions on how to make an explosive device and transferred USD 300 via the money transfer

system to purchase the necessary components. With a view to aid in terrorist activities, N. purchased components and parts for the fabrication of an explosive device and its subsequent transfer to terrorists, but his actions were timely suppressed by the intelligence services. The court found L. guilty of financing terrorist activities and aiding in the fabrication of an explosive device and sentenced him for the totality of the crimes committed to imprisonment for a term of 5 years.

558. The competent authorities demonstrated awareness of other TF typologies (e.g., hawala, fundraising in social networks, under the guise of charitable activities, etc.), as well as methods of detection of such crimes, but there were no facts of TF detection by the mentioned methods in the assessed period.

Case Study 9.7 (Fundraising for TF purposes under the guise of charity)

In the course of the police intelligence operations, the NSC revealed that "Muhajirun", "Salsail" and "Ansar" foundations created on the Internet raise funds under the guise of providing charitable assistance to needy Muslims, Syrian refugees, etc. A number of Kazakh nationals transferred money to bank card and other payment facilities numbers specified by the foundations. In the course of international information exchange it was found that A., who was on the international wanted list for terrorism and TF, had organized a clandestine network under the guise of charity. Members of the organized group under A.'s direction cashed out the money received from citizens and transferred it to ITOs "Islamic State" and "Jebhat al-Nusra". The activities of the organized criminal group were supressed by the Federal Security Service of the Russian Federation.

559. The criminal law establishes the exterritoriality of criminal liability for terrorist offences, according to which persons are liable under the CC regardless of the place where the offence was committed. Given the transnational nature of TF, implementation of this principle is essential to ensure unavoidability of liability. The country provides case studies of prosecution and conviction of persons who have committed TF offences in foreign jurisdictions.

Case Study 9.8 (TF in foreign jurisdictions)

In the course of the check into the involvement in terrorist activities of individuals repatriated to Kazakhstan from the terrorist activity zone, joint activities of the FMA and NSC allowed to establish that Kazakh national Yu. transferred 300 USD to the Republic of Azerbaijan via money transfer system in 2013 as financial assistance to O. designated in Rosfinmonitoring's list of persons involved in terrorist activities. In 2014, Yu., an adherent of destructive religious movements, with the intention of participating in the activities of ITO "DAISH" and financing terrorist activities, sold her owned house and land in Kazakhstan and received USD 20 thousand on her card account. Through Turkey, Yu. travelled to Syria, where she participated in the activities of the terrorist organization by providing medical assistance to fighters, underwent terrorist training, mastered firearms skills and took Shariah training courses. She gave the bank card to ITO member G., who cashed out the funds and used them for terrorist activities. In 2019, Yu. was taken captive and subsequently returned to Kazakhstan. The court found Yu. guilty of financing terrorist activities (both in Kazakhstan and Syria) and participating in a terrorist group and sentenced her for the totality of the crimes committed to imprisonment for a term of 8 years.

560. For detecting and suppressing terrorist and TF offences, the competent authorities actively use the mechanisms of international cooperation, which is carried out both at the operational level (through exchange of operational information, conducting joint special operations, suppression of facts of entry/exit of persons involved in the ITO) and as part of pre-trial investigations of criminal cases (for more details, see IO.2).

Case Study 9.9 (international cooperation in detecting TF)

The NSC, together with the National Intelligence Service of the Republic of Korea, conducted a special

operation, during which A., a Kazakh national involved in the financing of ITO "Khatiba Tawhid wal Jihad", was identified and detained. In 2020, the court of the Republic of Korea sentenced A. for TF to imprisonment for a term of 1 year and 6 months and imposed a fine equivalent to USD 1 thousand.

561. Criminal proceedings fro TF-related cases were not terminated at the stage of the pre-trial investigation. There were only facts of interruption of pre-trial proceedings due to putting the persons involved on the wanted list (7), failure to identify the person to be prosecuted (5), for the time of execution of requests for mutual legal assistance in foreign jurisdictions (2). In the assessed period, 31 cases of TF offences were referred for consideration on the merits. At the same time, in 11 cases the actions of the offenders were qualified only under CC Article 258, in 20 cases - under CC Article 258 in the aggregate with other offences.

562. Statistical information of the Supreme Court on the number of TF cases considered and their outcomes is shown in the table.

Table 9.2. Number of examined TF cases and their outcomes (cases/ persons)

	2017	2018	2019	2020	2021	6 months of 2022	total
cases considered by courts of first instance	8/10	5/5	2/2	3/4	6/13	3/10	27/44
convictions	8/10	5/5	2/2	3/4	6/13	3/10	27/44
cases considered by appeal courts	2/2	1/3	1/1	1/1	1/1	1/7	7/15
upheld or overturned convictions	2/2	1/3	1/1	1/1	1/1	1/7	7/15

563. It follows from the above data that in all TF-related criminal cases the courts issued guilty verdicts, which were upheld upon verification of their legality and validity by higher courts and entered into legal force.

564. At the same time, by virtue of the AML/CFT Law provisions, the entry of a sentence for TF into legal force entails designation of the convicted person in the National List of persons involved in the financing of terrorism and extremism and the occurrence of all related legal consequences (for more details, see IO.10).

565. The information on the staffing levels of the prosecution authorities is confidential and is therefore not included in this report. However, the information provided to the experts made it clear that the available staffing capacity is sufficient to perform the assigned tasks. The information and analytical resources of the prosecution authorities, procuracy and courts demonstrated to the assessment team indicated a sufficient level of logistical support.

566. Besides that, the country pays considerable attention to the training and professional development of specialists in the field of countering terrorism and TF. Relevant training is provided at the Law Enforcement Academy under the GPO, NSC Academies, MIA and Border Academy. According to the NSC, in the assessed period, more than 2,500 national security officers received advanced AML/CFT/CPF training at the departmental Academy alone. Training events were also held at the Justice Academy to improve the qualifications of judges.

567. The counter-terrorism training curricula for officers are closed, but they were shown to the experts during the on-site mission, who made sure that they included training activities on countering and prosecuting TF. Criminal prosecution officers were also trained in other countries.

568. Thus, combating TF is carried out on a comprehensive and systemic basis. TF detection and prosecution is one of the activities of LEAs/SSAs in the field of counter-terrorism. LEAs and SSAs have the necessary human, material and technical and information and analytical resources. Operational capabilities of the FIU are actively used for the purpose of detecting TF. The absence of facts of termination of criminal prosecution for TF at the pre-trial stage, referral of criminal cases by prosecutors for further investigation and acquittals by courts indicate the proper quality of implementation of criminal proceedings and pre-trial investigations by the national security agencies.

569. At the same time, given that combating terrorist offences is also the responsibility of the EIS and MIA, the TF detection efforts by these LEAs should be intensified.

4.2.3. TF investigation integrated with – and supportive of – national strategies

570. The legal basis defining the national counter-terrorism policy is the National Security Strategy approved by the Kazakhstan Presidential Decree. For the purposes of implementing the Strategy, documents have been developed and approved that define specific areas of activity of counter-terrorism actors, such as the Special Plan for Countering, Neutralizing and Eradicating Destructive Movements; the Roadmap for Preventing and Avoiding the Spread of Destructive Religious Movements among Minors; and the Complex of Systemic Measures for Countering Religious Extremism and Terrorism.

571. The mentioned documents are confidential. However, as part of the on-site mission the experts were given the opportunity to get acquainted with departmental acts (in part) developed to determine the tactics and methods of action of competent authorities in implementing the state counter-terrorism policy. It follows from them that the authorities clearly understand the need to eliminate the financial basis of terrorism, which is why the identification of TF sources and destructive religious movements, ensuring the unavoidability of liability for TF is considered as an independent strategic objective of prosecution authorities.

572. Coordination of activities in the counter-terrorism sphere is entrusted to the NSC and is implemented through the Kazakhstan Anti-Terrorist Center composed of the heads of 20 government authorities. The competence of the ATC includes the formation and improvement of state policy and counter-terrorism legislation, development of practical measures for government authorities, coordination of activities of government authorities aimed at countering terrorism, forecasting of terrorist threats, introducing of international counter-terrorism experience. The ATC organizes the activities of the Republican Operational Headquarters for Combating Terrorism and coordinates 206 counter-terrorism commissions under the executive authorities.

573. The ATC meetings are held on a quarterly basis to consider topical issues related to the activities of government authorities. Two such meetings on the CFT issues were held in the assessed period. Based on the results of the meetings, decisions are made on the implementation of necessary measures to improve the activities of competent authorities in the area of combating terrorism and its financing, and the implementation of these measures is monitored.

574. Measures aimed at countering religious extremism and terrorism, deradicalization of the population, and, as a consequence, mitigating TF risks are implemented by the government authorities in a systematic and comprehensive manner, in cooperation with each other.

575. The CFT issues are also reflected in other strategic documents, including the AML/CFT Law, the Laws on Combating Terrorism and Extremism and others.

576. The NSC and other government authorities carry out a wide range of CFT activities as part of the Program of Cooperation of SCO Member States and the Program of Cooperation of CIS Member States in Combating Terrorism and Other Violent Manifestations of Extremism supported by the plans for their implementation developed and approved at the domestic level.

577. The country has demonstrated the results of international cooperation as part of these Programs and other international treaties in the field of combating crime and terrorism. In particular, according to information from foreign partners, 199 nationals of Tajikistan, Uzbekistan, Kyrgyzstan and other countries involved in terrorist, extremist and conventional offences were identified, detained and returned to foreign jurisdictions by the NSC.

578. The Kazakhstan has initiated a number of activities aimed at increasing the level of international cooperation on counter-terrorism issues. In particular, the country participated in the establishment of the Global Network against International Terrorism. At the UNSC meeting chaired by Kazakhstan, a draft Code of Conduct towards Achieving a World Free of Terrorism was presented. On Kazakhstan's initiative,

measures were taken by decision of the SCO RATS to improve cooperation between competent SCO bodies in detecting and suppressing terrorist financing channels.

579. Thus, the experts were convinced that countering terrorism and religious extremism are among the priorities of state policy both at the domestic and international levels. Measures have been taken to coordinate the activities of all the actors involved in counter-terrorism activities and ensure the level of their proper interaction. The activity of prosecution authorities on detecting, suppressing and ensuring unavoidability of liability for TF offences is a means of implementation of the state criminal policy and is an independent strategic objective in the counter-terrorism context as a whole.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

580. According to the criminal law, TF offences are categorized as serious crimes and are punishable by imprisonment for a term of 5 to 9 years, and with aggravating circumstances (group of persons by prior conspiracy, on a large scale, etc.) - by imprisonment for a term of 7 to 12 years. Confiscation of property and other kinds of additional punishments can be applied as additional punishment in the cases established by law.

581. Analysis of sanctions for other terrorist offences shows that, compared to sanctions for TF, more severe liability is imposed for an act of terrorism that caused death or other serious consequences (imprisonment for a term of 12 to 17 years with confiscation of property), an act of international or state terrorism (imprisonment for a term of 15 to 20 years with confiscation of property) and the establishment of a terrorist group (imprisonment for a term of 10 to 17 years with confiscation of property). Other terrorist manifestations (terrorist propaganda, participation in the activities of a terrorist group, etc.) are comparable to TF in terms of gravity and sanctions.

582. If the person is brought to criminal liability for TF offences and other offences, according to the established rules, punishment shall be inflicted to him for each of offences, and the final punishment shall be determined on an aggregate basis by absorption of less strict punishment by more strict one or by partial or full addition.

583. Statistical information on sentencing under CC Article 258 (including cases of conviction in the aggregate with other offences) is given in the table below.

Table 9.3. Criminal sanctions for TF

		2017	2018	2019	2020	2021	total
Convicted persons		10	5	2	4	13	**34**
Sentenced to imprisonment		10	5	2	4	13	**34**
incl.	for a term of up to 5 years	5	1	1	2	7	**21**
	for a term of 5 to 10 years	5	4	-	2	6	**17**
	for a term of more than 10 years	-	-	1	-	-	**1**
With confiscation of property		6	1	-	-	-	**7**

584. In general, the above case studies of judicial practice show that when determining the type and term of punishment for TF, courts properly assess the public danger of this unlawful act. The sentence of less than 5 years for 16 persons is due to the fact that the perpetrators committed TF offences before 2016 during the period of a more lenient sanction under CC Article 258 part 1 (3 to 7 years' imprisonment).

585. Confiscation of property as an additional punishment was applied to 20.6% of convicted persons. Most often confiscation was applied to instrumentalities of crime (cell phones, weapons and ammunition). The somewhat limited nature of confiscation and the absence of facts of confiscation of property intended for TF purposes are due to objective factors, which are analyzed in Core Issue 9.2.

586. According to the information provided by the country, there have been no repeat offences (recidivism) by persons convicted of terrorist offences and TF. In this regard, the experts conclude that, sanctions imposed on natural persons for TF offences are generally proportionate, dissuasive and effective.

587. There is no criminal liability of legal persons for TF in accordance with the principles of national law.

In the case of legal persons, only civil liability is provided for TF, with the only sanction being liquidation resulting in the confiscation of property.

588. According to the information provided, between 2017 and the first half of 2022, 88 organizations (foreign jurisdictions) were recognized by courts as extremist at the prosecutors' request. Since 2015, no organisation has been recognised as a terrorist organisation and accordingly there have been no instances of liquidation or confiscation of assets. Therefore, it was not possible to draw conclusions about the effectiveness of sanctions against legal persons.

4.2.5. Alternative measures used where TF conviction is not possible

589. In the course of the CIDA and pre-trial investigations, the prosecution authorities investigate all aspects of the offenders' unlawful activity for the purpose of their criminal assessment. If it is not possible to secure a conviction for TF and elements of another offence are established, prosecution for another unlawful act is pursued. Such offences most often include incitement of religious hatred or discord, terrorist propaganda or public calls to commit an act of terrorism and others, as well as conventional offences (possession of weapons, ammunition, theft, etc.). According to the GPO, in the assessed period, about 150 individuals were convicted under alternative articles of the Criminal Code, against whom it was not possible to prove TF.

590. The strength of the country is a set of preventive measures implemented in order to prevent the involvement of people in illegal activities and their radicalization. Such measures are implemented on the basis of the state programs on countering religious extremism and terrorism adopted by the government for a 5-year period.

591. The state program for 2018-2022 developed by the NSC contains a list of activities aimed at reducing the number of people who share extremist ideas, increasing the proportion of terrorist and other violent extremist acts supressed at the stage of preparation, increasing the level of preparedness to deal with the consequences of terrorist acts in Kazakhstan.

592. The government authorities responsible for implementing the program are the NSC, GPO, State Protection Service, Foreign Intelligence Service, FMA, ACA, MIA, Ministry of Defence, other ministries and agencies, as well as executive authorities. The agencies have developed plans for the implementation of the program and interagency agreements have been concluded on cooperation in its implementation.

593. A wide range of awareness-raising measures are being taken to deradicalize nationals and reduce the number of persons adhering to destructive radical movements. As a result of the measures taken, more than 7 thousand Kazakh nationals have been deradicalized.

594. The NSC, in cooperation with the MIA, carries out systematic work aimed at the deradicalization of those convicted of terrorist offences and serving their sentences in the penal institutions. Theological and rehabilitation organizations, including non-government ones, are involved in this work. A total of about 500 convicts have been deradicalized. Special efforts are made to exclude their negative impact on other convicts, as well as to prevent the commission of new offences after their release.

595. The NSC and MIA keep special preventive registers of persons who have served their sentences for terrorist offences and are prone to destructive religious movements, in respect of which a set of preventive measures is applied.

596. In the assessed period, there were no cases of repeated commission of similar offences by persons who have served their sentences for terrorist offences, which demonstrates the effectiveness of the measures taken.

597. In order to identify persons carrying out public terrorist appeal, acting to incite religious, national, racial hatred or discord, the Internet is constantly monitored and the possibility of blocking the unlawful content is actively used. In the assessed period, more than 700 thousand links to web resources and materials containing propaganda of extremism, terrorism and destructive movements were blocked.

598. For the purpose of reducing the number of Kazakh nationals involved in the ITO activities, Kazakh authorities implement the "Zhusan" operation to return such persons to the country. A total of 607 persons were returned to Kazakhstan under this operation, of whom 37 were men, 157 women and 413 children. All men and 22 women were prosecuted for terrorist offences, including three for TF, in line with the principle of unavoidability of liability. Regarding repatriated nationals who were not involved in terrorism, a package of measures was taken for their resocialization and reintegration. The number of Kazakh nationals involved in the ITO activities decreased twofold.

599. Kazakhstan is a permanent participant in the "Barrier" operation, which, based on risk profiles, collects and analyzes information on Kazakh nationals who meet such profiles and sends the relevant information to LEAs and CIS ATC. In the course of the "Barrier" operation, based on the analysis of financial transactions, 3,719 individuals were identified who transferred money from Kazakhstan to terrorist activity areas in the amount exceeding USD 15.5 million. Proactive information on 55 individuals was sent to LEAs and information on 22 individuals was sent by the FMA to competent authorities of foreign countries.

600. The combination of these and other preventive measures made it possible to stabilize the criminal situation in the country, reduce the threat of terrorist manifestations, and as a consequence, to some extent mitigate the TF risks in the assessed period.

Overall conclusion on IO.9

601. The country's authorities clearly understand the threat of international terrorism and the external and internal factors that contribute to the involvement of citizens in terrorist activities, among which the most relevant for Kazakhstan is the radicalization of the population through involvement in destructive religious movements and propaganda of terrorist ideas.

602. Countering terrorism and religious extremism is a priority of state policy integrated into national policy documents and implemented in a systematic and comprehensive manner both within the country and through cooperation with international partners.

603. Measures have been taken to coordinate the actions of all actors engaged in the fight against terrorism and to ensure a high level of cooperation among all government authorities and organizations.

604. TF detection and prosecution is one of the activities of LEAs/SSAs in the field of counter-terrorism. LEAs and SSAs have the necessary human, material and technical and information and analytical resources. Operational capabilities of the FIU are actively used for the purposes of identifying TF, and parallel financial investigations are conducted. National security authorities ensure the proper quality of the CIDA and pre-trial investigations into TF offences. The results of criminal prosecutions are consistent with the NRA findings and the country's risk profile.

605. At the same time, the activities of other LEAs engaged in combating terrorist offences should be intensified.

606. Considerable attention is paid to the training and professional development of staff in the field of combating terrorism and its financing, and the necessary training and methodological base is in place.

607. The sanctions applied by the courts to natural persons for TF offences are effective, fulfill the function of private and general prevention, that is, they are dissuasive and generally proportionate, since they are imposed taking into account the public danger of the act and personal background.

608. At the same time, the information provided did not allow to make a definitive conclusion about the nature of sanctions in relation to legal persons.

609. In cases where it is impossible to secure a conviction for TF, prosecution for other offences (if any) is applied.

610. The improvement of the criminal situation in the country, reduction of the terrorist threat level and, as a consequence, TF risk mitigation is to a certain extent facilitated by a comprehensive system of

preventive measures implemented purposefully and on an ongoing basis.

611. **Kazakhstan is rated as having a substantial level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

612. Kazakhstan has demonstrated its ability to implement targeted financial sanctions (TFS) in the context of the UNSC lists, the national list and, upon request of third countries, to take action to freeze assets pursuant to UNSCR 1373 and its successor resolutions. The expert assessors base their conclusions on their own assessment of the various elements of the system, as well as on discussions with the relevant authorities (FMA, NSC, MFA and General Prosecutor's Office), supervisory authorities and a number of obliged entities.

613. In 2020-2022, Kazakhstan introduced amendments to national legislative acts aimed at improving the mechanism of implementation of TF-related TFS in terms of compliance with the "without delay" principle. Regulations on TFS implementation procedures were approved just before the on-site mission. At the same time, Kazakhstan has been generally using a proper system for the implementation of TF-related TFS over the past few years.

4.3.1. Implementation of targeted financial sanctions for TF without delay

614. Kazakhstan implements TFS on the basis of two lists: (a) natural persons and terrorist organizations designated under UNSCR 1267/1989/2253 and 1988 and (b) natural persons and terrorist organizations identified and designated by Kazakh authorities (national list generated in compliance with UNSCR 1373).

615. The second list includes , inter alia, natural persons and entities that have been designated at the request of third countries and have not been prosecuted for terrorism, which is also consistent with the UNSCR 1373 provisions. The domestic regime of designation in the sanction list includes both terrorist and extremist activities as grounds.

Generating, updating, disseminating the List and applying TFS without delay

616. In accordance with the provisions of the Constitution of the Kazakhstan, international treaties, as well as other obligations of Kazakhstan (including the UNSC) are an inseparable part of the national legal system. MFA informs the competent authorities, including the FMA, of any changes in the lists via official channels. At the same time, in order to ensure the application of TFS without delay, Kazakhstan amended the AML/CFT Law [23] in 2020 to allow the FMA to receive the relevant UNSC lists directly from the official UNSC website. Besides that, in 2022, the FMA also amended its internal regulations to ensure that the list is fully automatically amended upon publication of the UNSC decisions (parsing). In case there are failures and (or) technical malfunctions in the system of automated information retrieving from the official website of the UNSC Committees, information on the update (inclusion/exclusion) is also received to the FMA's e-mail and the e-mail of the head and responsible officer of the FMA structural unit (the mechanism of information receipt by e-mail was also used before the transition to automatic information receipt from the UNSC website). At the same time, in accordance with the provisions of FMA Order 5, a responsible FMA employee is on duty, including on weekends and public holidays (see Criterion 6.4) according to the schedule approved by the First Deputy Head of FMA. The provisions of the Kazakhstan legislation regarding the implementation of TFS without delay (in terms of FMA employee on duty) have been applied since 2016 in accordance with the Order 6 dated 29.01.2016. The information received through the channels of the Kazakhstan MFA continues to be used, but is an additional source of verification of the already listed information and application of TFS.

617. The time taken by Kazakhstan to publish updates to the TF-related UN sanction lists is given in Table 10.1.

618. The national list is generated by the responsible FMA officer within a few hours of the receipt of

[23] RK Law No. 325-VI dated May 13, 2020 (entered into force on November 15, 2020).

information from the Committee on Legal Statistics and Special Accounts and/or GPO, as well as the request of a competent authority of a foreign country.

619. Thus, Kazakhstan, on average, publishes the lists on its official website and send information to the obliged entities electronically via the personal account and e-mail within a few hours. Actually, in most cases, it takes no more than 30 minutes to publish the lists (additions, amendments or removals). The launch since 2022 of new "Web-SFM" portal on the basis of the FMA and its capabilities allows to generate notifications sent to the personal account and e-mail addresses of each obliged entity. Besides that, the FMA has built a system of sending to obliged entities an information message via available means of communication (chats/groups in messengers) in case of changes (inclusion/exclusion) in the lists of entities and individuals involved in the financing of terrorism and extremism.

620. The publication of the lists is the legal basis for the obliged entities to apply measures to freeze the funds and other assets of persons designated in the relevant UN sanction lists, as well as the occurrence of liability for violations of these requirements. In 2021, the AML/CFT Law was amended[24] to establish requirements for the obliged entities to freeze assets within 24 hours of publishing the list on the official FMA website (previously - not later than one business day). Despite the time limits specified in the law, in practice this requirement is implemented in less time. The expert assessors were provided with a sufficient number of examples of relevant documents, printouts and scans, time details, which allowed them to conclude that TF-related TFS are implemented without delay.

Table 10.1. Publication by the Kazakhstan of updates to the UN sanction lists (in accordance with UNSCRs 1267/1989/2253 and 1988)

UNSC Resolution	Date of making amendments to the UNSC list	UNSC Decision	Publication on the FMA website	Time for publication (days)
1267/2253	27.05.2022	6 entries were amended	27.05.2022	<1
1267/2253	01.04.2022	2 entries were amended	01.04.2022	≤1
1267	07.03.2022	1 entry was added	07.03.2022	<1
1267/2253	03.03.2022	5 entries were removed	04.03.2022	≤1
1267/2253	24.01.2022	1 entry was removed	25.01.2022	≤1
1267/2253	17.01.2022	3 entries were removed	18.01.2022	≤1
1267	03.01.2022	5 entries were removed	04.01.2022	≤1
1267/2253	30.12.2021	2 entries were added	31.12.2021	≤1
1267	29.12.2021	62 entries were amended	30.12.2021	≤1
1267/2253	21.12.2021	1 entry was added	22.12.2021	≤1
1267/2253	24.11.2021	1 entry was added	24.11.2021	<1
1267/2253	06.09.2021	1 entry was removed	07.09.2021	≤1
1267/2253	17.06.2021	1 entry was added	18.06.2021	≤1
1267/2253	06.04.2021	1 entry was amended	07.04.2021	≤1
1267/2253	23.03.2021	8 entries were amended	24.03.2021	≤1
1267/2253	23.02.2021	92 entries were amended	24.02.2021	≤1
1267/2253	19.02.2021	2 entries were removed	20.02.2021	≤1
1267/2253	08.10.2020	1 entry was added	09.10.2020	≤1
1267/2253	10.09.2020	11 entries were amended	11.09.2020	≤1
1267/2253	29.03.2019	6 entries were amended	30.03.2019	≤1
1267/2253	22.03.2019	1 entry was added	23.03.2019	≤1
1267/2253	13.03.2019	1 entry was amended	14.03.2019	≤1
1267/2253	28.02.2019	1 entry was added	28.02.2019	<1
1267/2253	08.02.2019	4 entries were added	09.02.2019	≤1
1988	30.01.2019	2 entries were amended	31.01.2019	≤1
1988	10.04.2018	1 entry was amended	11.04.2018	≤1
1988	16.02.2017	1 entry was removed	17.02.2017	≤1

[24] RK Law No. 73-VII dated November 18, 21 (entered into force on January 19, 2022).

UN sanction lists

621. Kazakhstan applies an interagency approach to the listing of natural persons and terrorist organizations in accordance with UNSCRs 1267/1989/2253 and 1988 (and their successor resolutions). Interaction on designation in the UN sanction list is coordinated by the Ministry of Foreign Affairs of Kazakhstan in accordance with Joint Order No. 1009/dsp, which was reviewed by the assessment team during the on-site mission. The order regulates the interaction between the NSC, GPO and FMA of Kazakhstan prior to the submission of a proposal for designation of a person or terrorist organization to the relevant UNSC Committee by the MFA of Kazakhstan. Before sending a proposal to the UN Committee based on the proposals of the competent authorities, including the NSC, FMA and other law enforcement authorities, the MFA may conduct additional consultations to work out the designation details and make sure that the proposal complies with the rules of the UN Committees (such as templates, terms of reference, etc.), and, if necessary, request additional information.

622. At the same time, despite the existing mechanism, Kazakhstan has not proposed in the assessed period any person or organization for designation in the sanction lists generated by the UNSC Committees. The competent authorities justify the absence of proposals for designation of individuals and entities in the UN sanction lists by the fact that the persons designated in the domestic lists are either imprisoned in Kazakhstan or occupy ordinary positions in the ITO hierarchy, and as such pose no threat to the international community, which makes the proposal for designation in the international list unnecessary.

National sanction lists

623. Kazakhstan provides for the following conditions for a decision to designate an individual or entity in the national list generated in accordance with UNSCR 1373: (a) the existence of criminal prosecution for involvement in terrorist activities; (b) a court decision or sentence (including a foreign one); (c) lists of organisations and individuals involved in terrorist and extremist activities compiled by the GPO, based on data from law enforcement and specialised agencies of the Kazakhstan; (d) requests from third countries. At the end of September 2022, the national list contained 1267 terrorists and 89 terrorist organizations. Besides that, 266 extremists were designated in the national list.

Table 10.2. National sanction lists of terrorists and terrorist organizations (designated/year)

	2017	**2018**	**2019**	**2020**	**2021**	**9 months of 2022**
Terrorists	234	150	99	84	86	53
Terrorist organizations	5	4	0	0	0	0

624. Kazakhstan also designates natural persons and entities in the sanction list for extremist activities with the application of measures to freeze funds or other assets. Although beyond the scope of this assessment, the table below is provided to describe the overall situation in the country.

Table 10.3. National sanction lists of extremists and extremist organizations (designated/year)

	2017	**2018**	**2019**	**2020**	**2021**	**9 months of 2022**
Extremists	51	40	36	17	70	32
Extremist organizations	0	0	0	0	0	0

Table 10.4. Amount of assets frozen (KZT/ unit)[25]

	2017	**2018**	**2019**	**2020**	**2021**	**9 months of 2022**
Total	46 017 042 ($ 141 590)	75 824 428 ($ 199 538)	76 997 410 ($ 202 093)	80 949 880 ($ 192 738)	82 786 240 ($ 192 080)	82 833 024 ($ 184 073)
Frozen on terrorist financing offences						
The sum of	44 847 209	46 934 863	47 092 136	50 566 409	50 901 424	50 948 209

[25] KZT/USD exchange rate for 2017 is 325 KZT, 2018 - 380 te KZT nge, 2019 - 381 KZT, 2020 - 420 KZT, 2021 - 431 KZT, 2022 - 450 KZT.

	($ 137 991)	($ 123 513)	($ 123 601)	($ 120 396)	($ 118 101)	($ 113 218)
Real estate	316	357	384	412	422	426
Movable property	105	129	0	131	136	0
Frozen on extremist financing offences						
The sum of	1 169 833 ($ 3 599)	28 889 565 ($ 76 025)	29 905 274 ($ 78 492)	30 383 471 ($ 72 342)	31 884 815 ($ 73 979)	31 884 815 ($ 70 855)
Real estate	40	62	81	90	101	114
Movable property	24	34	35	35	44	50

625. With regard to requests from foreign countries in accordance with UNSCR 1373, the FMA of Kazakhstan is the authorized body to consider such requests. The FMA also sends requests to foreign countries. Using this mechanism, Kazakhstan has responded to 3 requests for 1,183 individuals from the Russian Federation and the Kyrgyz Republic. The following requests were considered by the FMA within 1 day of their receipt.

Table 10.5. Information on the persons included in the list based on requests from third countries

	2017	**2018**	**2019**	**2020**	**2021**	**9 months of 2022**
Russian Federation	419	0	0	586	0	0
Kyrgyz Republic	0	0	0	0	0	178

626. After completing the generation of the list of specified persons, the FMA publishes it on its Internet resource for the obliged entities to take measures to freeze transactions with funds and (or) other assets within a period of up to fifteen calendar days. During this period the FMA shall coordinate the list with the competent authorities of the Kazakhstan. If the competent authorities refuse approval, information on the entities and individuals designated in the this list shall be removed from the FMA Internet resource and the requesting party shall be informed to that effect.

627. If the competent authorities confirm the sufficiency of grounds in accordance with AML/CFT Law, Article 12, Par. 4, after fifteen calendar days, the FMA shall take measures to designate specified persons in the list of entities and individuals involved in the financing of terrorism and extremism.

628. There were no facts of freezing of funds upon the requests received from foreign countries due to the absence of accounts and assets of the requested persons in the territory of the Kazakhstan.

629. Regarding outgoing requests to authorities of other countries, the FMA has sent 2 requests in the assessed period regarding 159 individuals convicted under terrorist articles, involved in TF or suspected of such activities. The above requests were sent to the EAG member states (Republic of Belarus, Kyrgyz Republic, Russian Federation, Republic of Tajikistan and Turkmenistan). The expert assessors note that Kazakhstan does not systematically send proposals to third countries, other than CIS countries, for designation in national lists pursuant to UNSCR 1373. However, the competent authorities of Kazakhstan provided information during the on-site mission that the absence of such requests is due to the fact that persons on the national list do not have accounts or property in countries outside of the CIS.

De-listing

630. The grounds for de-listing from the national terrorist list are similar to those for listing. Between 2017 and September 2022, Kazakhstan de-listed 198 natural persons from its national terrorist list, representing approximately 37% of the total number of de-listed persons.

Table 10.6. Information on de-listed persons

	2017	**2018**	**2019**	**2020**	**2021**	**9 months of 2022**
Terrorists	11	13	4	15	58	97
Extremists	17	31	45	63	133	36
Terrorist organizations	0	0	0	0	0	0
Extremist organizations	0	0	0	0	0	0

Interaction with the obliged entities

631. It should be noted that the obligation to apply TF-related TFS does not apply to all natural and legal persons, but only to the obliged entities and certain government authorities and organizations, since there are no provisions in the legislation of the Kazakhstan directly stipulating liability for violation by all natural and legal persons (except FIs, DNFBPs and VASPs) of the prohibition on providing funds and other assets to designated persons.

632. To improve understanding of the TFS requirements among the obliged entities, the FMA provides an explanation of the legal regulation of this issue on its official website. Besides that, information on the application of TFS is communicated to the obliged entities through personal accounts. The FMA has also published on its official website memos for the obliged entities, which also contain information on TF-related TFS requirements. In 2020, the FMA developed recommendations for government authorities and obliged entities to freeze transactions with funds and (or) other assets of designated persons[26]; in 2021 developed and disseminated recommendations for the obliged entities (microfinance organizations, pawnshops)[27]; also in 2021, the FMA issued recommendations for insurance companies and notaries).

633. As noted in IO.4, those obliged entities that met with the assessment team demonstrated a good understanding of their obligations to apply TF-related TFS. Larger obliged entities have effective sanctions enforcement controls, using, *inter alia*, automated reconciliation to the list and commercial databases. All the obliged entities have access to a personal account on the FMA official website through which they receive updated lists. Smaller obliged entities have less sophisticated controls, and some of them have to check their client databases manually.

634. In case of identifying the persons designated in the list when establishing business relationships, all the obliged entities refuse to establish business relationships and send a report to the FMA. If designated persons are identified among active clients, the obliged entities freeze funds and also send a report to the FMA. During the on-site mission, the expert assessors were provided with case study of a false positive (Case Study 10.1).

635. All the private sector entities that met with the assessment team during the on-site mission were made aware of their obligation to suspend a transaction for up to 16 days in case of suspicion (suspension for 15+1 days) followed by sending an STR to the FMA for analysis and confirmation or denial of the grounds for suspicion. If suspicions were confirmed, transactions were blocked.

Case Study 10.1 (TFS false positive)

A client (A.V. Lee, born 1987) approached the credit institution. During the identification process, an officer of the credit institution identified a partial match between the customer's identification data and the person designated in the TF list (A.V. Lee, born 1989). The credit institution suspended the transaction and sent a report to the FMA to confirm the information as to whether the person was designated or related to the designated person.

The FMA analyzed the information received and authorized the transaction on the basis that the customer had a different IIN, and given the fact that the person designated in the TF list was in prison at the time of the transaction, which was also confirmed by information from the convicted persons database.

636. One of the big challenges to effective TF-related TFS implementation is whether FIs/DNFBPs are correctly identifying the customer's ultimate BO or parties to the transaction. As the assessors were able to verify during the on-site mission, the obliged entities understand their obligations to identify the customer's BO. However, there are some deficiencies with respect to identifying the customer's BO (see IO.4) that may have reduce the effectiveness of the measures applied. At the same time, this is mitigated by the fact that the obliged entities do not use a formal approach to BO identification. Information provided directly

[26] RK FMC No. KFM/4300-vn dated September 30, 2020.
[27] No. 0/152-vn and No. 0/153-vn dated March 12, 2021.

by customers as part of the CDD process is verified using various commercial databases. In cases of doubt as to whether the person with the controlling interest is the BO, the obliged entities confirm this information during the analysis of the customer's transactions. In some sectors, the obliged entities have recorded cases of refusal to establish a business relationship when the ultimate BO cannot be identified.

637. As noted in IO.3, regulatory and supervisory authorities, including the ARDFM and FMA, conduct on-site and off-site audits with respect to the application of TFS. No violations of the requirements for the proper application of TFS have been identified during such audits.

4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations

638. In the Kazakhstan, a non-commercial organization (non-profit organization) is understood as a legal entity, which does not have as its main purpose the generation of income and does not distribute received net income between the participants, which is regulated by the Law of the Kazakhstan on Non-Profit Organizations (hereinafter the Law on NPOs). According to the Law on NPOs, they can be established in the form of: institution, public association, joint stock company, consumer cooperative, foundation, religious association, association (union) of legal entities and in any other form stipulated by legislative acts.

639. Thus, in Kazakhstan, NPOs in the classical sense can include public associations (with the exception of political parties, trade unions and religious associations), foundations (with the exception of state foundations), associations of legal entities and private institutions.

Table 10.7. Breakdown of registered non-profit organizations by legal form (in percent)

	2018	2019	2020	2021	6 months of 2022
Total	**100**	**100**	**100**	**100**	**100**
including:					
public associations	35,01	35,60	35,63	63,42	42,375
institutions	10,69	10,41	10,28	5,99	3,125
non-profit joint-stock companies	0,16	0,17	0,18	0,13	0
consumer cooperatives	14,02	13,54	13,15	8,34	1,875
foundations	21,24	21,74	22,29	7,73	36,25
religious associations	2,18	2,07	1,99	0,00	0,5
associations of legal entities	4,97	5,00	5,02	3,77	7,875
Other non-profit organizations	11,72	11,46	11,46	10,63	8

640. State registration of legal persons that are non-profit organizations and record registration of their branches and representative offices is carried out by judicial authorities.

641. According to the Ministry of Justice, as of January 1, 2022, there were over 22 thousand NPOs registered (Chapter 1, Table D), including 10207 public associations; 6325 foundations; 3603 religious associations, covering 18 confessions; 68 branches and representative offices (stand-alone units) of foreign and international non-profit organizations operating in the Kazakhstan. The bulk of NPOs work in 18 areas of activity (youth, pensioners, protection of vulnerable groups, environment, health, culture, sports, protection of historical and cultural heritage, etc.).

642. According to the information provided by the country, 17,000 of the total number of registered NPOs actually operate in Kazakhstan, with the majority of them established to pursue the narrowly defined interests of a certain circle of people in order to achieve their goals that are not contrary to the law. For example, public interest associations of gardeners, dog breeders, medical workers, parents of schoolchildren, technical workers, members of sports clubs and educational organizations, etc.

Table 10.8. Information about the number of registered non-profit organizations

	2017	2018	2019	2020	2021	6 months of 2022
Public associations	731	775	886	715	943	339

Institutions	94	108	126	71	89	25
Non-profit joint-stock companies	-	-	-	4	2	-
Consumer cooperatives	143	136	159	112	124	15
Foundations	121	133	153	85	115	290
Religious associations	7	15	10	0	0	4
Associations of legal entities	77	85	119	41	56	63
Other non-profit organizations	3	3	17	323	158	64

643. The registration authority may refuse to register NPO in cases established by law. In particular, a person included in the TF/PF list cannot be a founder (member) of a non-profit organisation.

Table 10.9. Information on refusals to register NPOs.

	2017	**2018**	**2019**	**2020**	**2021**
Violation of the procedure for establishment, re-registration and reorganisation of a legal entity established by legislative acts of Kazakhstan, inconsistency of constituent documents with the law of Kazakhstan.	114	123	175	198	254

644. The authorized body responsible for the creation of an information database intended for ensuring transparency of NPOs' activities and informing the public about them (hereinafter in this section the Database) is the MISD. The direct work is carried out by The Civil Society Committee of the MISD. The assessors verified that MISD has sufficient human and physical resources to conduct effective NPO monitoring. In addition, when maintaining the Database, the MISD uses an automated risk management system to identify, monitor and control high-risk NPOs.

645. Kazakhstan is making certain efforts to assess and monitor the NPOs sector for potential misuse for TF purposes. The country has measures in place to prevent NPOs exposed to such risk from registering, terminating and liquidating them, as well as sanctions for non-compliance by NPOs with the relevant control requirements of the state.

646. In 2022, a risk assessment of the misuse of NPOs for terrorist financing was conducted. The risk of NPOs being used in terrorism financing schemes is assessed to be medium, as foreign funding does not come from high-risk countries. The reason for this is that, as a rule, Kazakhstan funds are used to implement various types of NPO projects, NPOs are required to submit reports, and there is a systematic mechanism of domestic cooperation that allows NPOs to monitor their activities.

647. NPOs outreach, engagement, and oversight of at-risk NPOs are generally based on the NRA and TF SRA findings, according to which the medium risk level is assigned to charitable and religious organizations. In the assessed period, there were no facts of involvement of NPOs in TF activities. The FMA prepared CFT Recommendations for the NPOs sector. In August 2022, the FMA approved the Methodology for sectoral risk assessment of the NPOs sector misuse for terrorist financing purposes; however, it is not possible to assess its application, given the short period of validity (adopted 3 weeks before the on-site mission).

648. The use of disguised sources of terrorist activities funding under the façade of legal activities of various charitable foundations or fundraising through Internet sites - crowdfunding - has become widespread. During the inspection it was found that the "Muhajirun", "Salsabil" and "Ansar" foundations created on the Internet raised money under the façade of charity activities to help needy Muslims, Syrian refugees, Muslim students studying in Europe and to support building wells in Africa (Case Study 9.7). The said fundraising was mainly focused on the post-Soviet space, including Kazakhstan, with a number of its citizens providing such charity through money transfers. The offenders published the details of bank card and various payment instruments in social networks and messenger chats, where, using the aforementioned foundations, they raised funds, cashed them out and transferred to terrorist organizations.

649. Pursuant to current national regulatory rules, reports are submitted to the Database by NPOs annually by March 31 of the year following the reporting period, using the approved form. Besides that, in order to

excersize control over the activities of a non-profit organization, NPOs are required to keep accounting records and submit primary statistical data to the National Statistics Bureau of the Agency for Strategic Planning and Reforms and the State Revenue Committee of the Ministry of Finance of the Kazakhstan in the manner prescribed by the Kazakh legislation. NPOs carrying out activities using the funds donated by foreign countries, international and foreign organizations, foreigners and stateless persons shall submit a report on the use of these funds to the state revenue authorities. At the same time, NPOs interviewed during the on-site mission explained that relevant information, including information submitted to the Database, is provided mainly by NPOs involved in the processes of receiving state grants, as the availability of such information is mandatory in such cases.

650. At the same time, the country's authorities provide data that more than 10,000 NCOs in Kazakhstan are created on the principle of an association of citizens based on interests, such as gardening, dog breeding, owners of apartment buildings, parents of schoolchildren, etc. Most of them are not active and are not involved in any socio-political processes; therefore, the authorities' control is focused on those NCOs that are the most risky in terms of terrorist financing and other criminal activities. To this end, audits are conducted. For example, in 2020, the SRC audited more than 20 Kazakhstani NPOs and branches of foreign NPOs suspected of misuse of funds provided by international donors and embassies.

651. During the on-site mission, the assessment team was shown the mechanisms of control over NPOs, including their registration. For example, the database of NPOs of the Kazakhstan is integrated with the main databases of the Ministry of Justice of the Kazakhstan (State Database of legal persons and natural persons). When citizens register NPOs, all primary data are checked by the justice authorities for compliance with legislation and validity (charter, protocols, copies of IDs and passports, address of the LP, signatures, etc.). These data are entered into the Electronic digital signature (EDS) of the first head of the NPO who can submit reports only with a valid EDS. Thus, when submitting information to the NPO database, the head is authenticated by means of EDS key that excludes unreliability of primary data. When the first head changes, he/she must obtain a new EDS through the National Certification Authority (NCA) of the Kazakhstan (pki.gov.kz). In the NPO database, the operator has the opportunity to update and verify the valid registration data within 20 working days from the date of its change.

652. Also, the financial reporting form in the database of NPOs is synchronized with the tax reporting of NGOs in SRC. At the same time, the database of NPOs is certified by the State Technical Service of the Kazakhstan for information security in order to exclude third-party interference and external threats.

653. At the same time, it is of some concern that the authorities in the interviews, as well as in the Report on vulnerability of legal persons and arrangements to involvement in ML/TF schemes, noted the failure to submit or late submission of the approved reporting by NPOs, which requires additional measures to improve efficiency in this area.

Table 10.10. Information about NPOs' breaches of the activity reporting

Period	Number of protocols	Court decisions
2017	40	40
2018	47	47
2019	61	60
2020	55	55
2021	58	58

654. At the same time, the experts positively assess the country's understanding of NPOs' failure to submit reports as a factor increasing the NPOs sector risk in terms of their possible misuse for terrorist financing purposes. In order to mitigate this risk, the government authorities, as well as the authorized body, carry out awareness-raising work with representatives and senior executives of NPOs.

655. The MISD holds workshops with NPOs to explain the requirements of TF legislation and international standards. As a rule, such workshops cover the issues of combating both ML and TF.

656. Thus, the MISD coordinates the activities of regional religious awareness-raising groups (hereinafter

referred to as ARG) in the field. This work is carried out through the efforts of 236 regional ARGs with 2,921 lecturers. As part of awareness-raising activities on religious issues, meetings, discussions and seminars are held with various categories of citizens to discuss the main directions of State policy in the sphere of religion, the promotion of the principles of secularism and the inadmissibility of the use of religion for destructive and radical purposes. In 2022, for example, more than 36,000 events in various formats were held with the participation of ARG members, reaching more than 1.6 million people.

657. In addition, every year MISD implements the project "Organization and conduct of awareness-raising work in the regions" (in 17 regions) to improve religious literacy of the population and prevent religious extremism. For example, 229 events were held under the project in 2022, covering 17 regions, 27 cities and 17 rural districts and reaching more than 9,000 people.

658. There is also a project to organise and carry out awareness-raising activities among women believers (in 8 regions). As part of the project, 170 ARG events were held in 2022, covering 8 regions, with the participation of 5,869 women.

659. On a quarterly basis, meetings of representatives of religious associations are held in Kazakhstan to discuss topical issues affecting the activities of religious associations, including explanations of legislation on preventing the financing of extremism and terrorism.

660. As part of providing practical assistance to heads of religious associations, representatives from the FMA are systematically invited to relevant meetings to inform those present about the main ways and mechanisms of financing terrorism and extremism, as well as measures to prevent them. In addition, assessment reports on the national system for combating money laundering and terrorist financing are reviewed at such meetings, and NPO proposals for amendments to legislation on state control of NPO financial activities are collected.

661. Similar meetings are organised by local executive bodies at the regional level, where representatives of financial monitoring units are also invited.

662. In addition, the Kazakhstani authorities provide information on the risks of using NPOs to finance terrorist activities through the publication of various handbooks, guidance documents, and memos. For example, in 2021, a methodological handbook "Analysis of the Activities of Religious Associations in the Republic of Kazakhstan" was published and brought to the attention of NPOs, with section 7 devoted to the analysis of charitable and sponsorship assistance, the relevant Memo to NPOs (No. 22-01-22/131 dated 09.03.2022), as well as a questionnaire for representatives of the non-profit sector at risk of use for terrorist financing and proliferation of weapons of mass destruction (No. 22-01-22/395 dated 27.07.2022), which received answers later submitted in FMA.

663. Moreover, the activities were implemented as part of the State Program on Countering Religious Extremism and Terrorism in the RK for 2018-2022. Paragraph 4 of the Action Plan for its implementation provides for awareness-raising activities among various categories of citizens, including religious institutions, on countering the risks of terrorist financing.

664. At the same time, since 2020 the project "Religious ministers carry out educational work to prevent the spread of ideology of destructive and radical religious movements", which addresses issues of counteraction to TF is being implemented in Kazakhstan. The project involves 1,319 clergymen from mosques in all regions of the Republic, except for cities of national importance. In addition to current issues in the religious sphere, meetings with parishioners and believers in general discuss "Religious extremism and terrorism - epidemic of the century", "Ways to prevent religious extremism and terrorism", "Religious literacy - main struggle against extremism" and other topics.

665. In total, more than 5,000 events are held each month to raise awareness about countering terrorist financing and related threats. The coverage of the events is about 66,000 people per month, with a total of more than 740,000 people annually.

666. At the same time, during the on-site mission some NPOs demonstrated a lack of awareness about the

risks of their involvement in TF, suggesting that there is a need to improve the mechanism for informing NPOs accordingly, in addition to conducting training activities.

667. In addition, workshops on AML/CFT legislative amendments are held by local executive bodies, which are constantly informed by the MISD (for example, in 2022 the relevant meetings were held by the Akimat of Shymkent city, Zhambyl, East Kazakhstan and Atyrau areas). The positive point is that in some cases the information and awareness-raising events are attended by representatives of the FIU and law enforcement authorities.

668. In view of the information received, the assessors believe that the supervisory authority for NPOs (MISD) applies measures of control (monitoring) of NPOs, but such measures are more of a unified approach to the supervision and monitoring over NPOs, although comply with the risk-based approach.

669. If a charitable organization or religious association suspect their misuse for the purpose of terrorist financing, they are required to send the relevant information to the authorized body. At the same time, during the on-site mission, the NPOs who participated in the interview were unable to explain the mechanisms of such reporting, as well as to name exactly which authority should be informed. Besides that, some NPOs demonstrated a lack of knowledge of the FMA's powers, which is not generally indicative of a deficient NPO monitoring and oversight system, nor is it indicative of inadequate interaction between the FMA and NPOs, given the amount of training for NPOs in which FMA representatives participate meaningfully.

670. The experts believe that the representatives of NPOs who participated in the meetings sufficiently understand the vulnerability of organizations to being misused for TF, but do not pay due attention to the targeting of the assistance they provide, believing that this problem is solved by the bank when opening an account and issuing a client's bank card, to which the funds are transferred to the person in need.

671. The MISD monitors the activities of NPOs. Representatives of the agency noted that the prioritization of monitoring of specific NPOs is based on two factors: the activities of concern and the volume of incoming funds. However, no enhanced supervisory or monitoring measures are applied to NPOs that require mandatory application of TF risk mitigation measures due to the inappropriateness, in their opinion, of interfering with the ongoing activities of NPOs.

672. The MISD representatives did not indicate whether and how they use the data provided by law enforcement authorities on the findings of the police intelligence activities against individual participants and organizers of NPOs, analysis of NPO-related STRs received by the FIU, etc.

673. According to representatives of NPOs, there is no direct interaction with the FIU and law enforcement agencies. At the same time, the country has built interagency cooperation between supervisory and law enforcement authorities, which generally allows, if necessary, to collect and verify information about the activities of NPOs and their possible involvement in TF in a timely manner, as well as to exchange it, including at the international level. No facts of NPOs involvement in the TF activities were identified in the assessed period. No NPO-related requests, including information about the dubiousness of foreign donors of NPOs, were received via international cooperation channels.

674. The main focus of the competent authorities in working with public foundations and religious organizations and monitoring their activities is to ensure the transparency of fundraising and accounting of incoming donations.

675. With this in mind, the assessors believe that the most important issue, namely the targeted use of the financial assistance provided, is actually neglected by all actors. The MISD is limited only to NPOs' reports on the receipt and expenditure of funds. NPOs themselves consider control of target use impossible due to the lack of appropriate powers, relying on the checks conducted by banks when opening an account. Factors mitigating the risk in this situation are the insignificant amount of assistance provided and its provision in non-cash form.

4.3.3. Deprivation of TF assets and instrumentalities

676. Kazakhstan has demonstrated that it deprives terrorists, terrorist organizations and terrorist financiers of their existing assets and instrumentalities of crime by using various methods, including designation and freezing of funds. Small overall amount of frozen assets is consistent with the risk profile, as those to whom asset freezing measures are applied tend to use their own sources of income rather than outside funding, are from relatively poor segments of the population with limited funds available. As for the confiscation of funds and property intended for TF, the total amount, although small, is also consistent with the country's risk profile.

677. As noted above, Kazakhstan actively uses the authority to designate individuals and entities in the national sanction lists to deprive terrorists and terrorist organizations of their assets. The total amount of frozen funds in the assessed period is USD 721 thousand and 2,317 objects of immovable property.

678. It should be noted that the freezing of funds and other assets of designated individuals and entities is carried out by both obliged entities and government authorities, as well as organizations involved in the registration of rights to movable and immovable property.

Table 10.11. Amount of frozen assets of designated entities and individuals (thousands of USD/items of property)

	2017	2018	2019	2020	2021	9 months of 2022	Total
Funds	130	123	123	120	115	110	**721**
Immovable property	316	357	384	412	422	426	**2317**
Movable property	105	129	0	131	136	0	**501**

679. In the assessed period, there were also facts of providing access to frozen assets that are necessary for basic expenses of persons included in the TF list. In the period from 2107 to September 2022, access to frozen assets was granted to 126 persons for a total of USD 17,738.

Table 10.12. Amount of accessed funds of designated entities and individuals (USD)

Period	Number of persons	Amount
2017	5	310
2018	24	4 016
2019	21	3 147
2020	32	3 238
2021	24	2 644
9 months of 2022	20	4 383
Total	**126**	**17 738**

4.3.4. Consistency of measures with overall TF risk-profile

680. According to the 2021 NRA, TF risk in the Kazakhstan is medium. During the on-site mission, the experts were able to verify that TF-related NRA findings correlate with the opinion of Kazakh competent authorities regarding the country-specific risks in the context of terrorist activities threats (see IO.9).

681. The measures taken by Kazakh authorities are generally consistent with the overall TF risk profile of the country. As noted above, Kazakhstan actively populates the lists of terrorists and terrorist organizations in accordance with UNSCR 1373. However, compared to this data, Kazakhstan does not make use of the available mechanism for adding terrorists to UN lists, while making such proposals could lead to asset freezing requirements being extended to all UN member states. Besides that, according to the expert assessors, the country should also more actively apply measures for mutual freezing of assets of persons designated in the national lists, not only in cooperation with EAG member states, but also with other countries, where terrorist assets could be located.

682. The assessment team reviewed the data provided to them on the availability of resources for the competent authorities to carry out functions related to the implementation and application of TFS. Based on the interviews and provided materials, the expert assessors concluded that the measures for freezing assets of terrorists and terrorist organizations as well as confiscating property that was misused for TF

purposes were proportionate.

683. Kazakhstan applies measures of control (monitoring) of NPOs, but such measures are more of a unified approach to the supervision and monitoring over NPOs, although comply with the risk-based approach.

Overall conclusion on IO.10

684. Kazakhstan demonstrates its ability to apply TFS in accordance with the UN sanction lists, the national list and in response to requests of third countries to take actions to freeze assets pursuant to UNSCR 1373. Despite the amendments to the regulatory legal framework of the Kazakhstan in 2020 aimed at enshrining at the statutory level the mechanisms and procedures for compliance with TFS requirements by the obliged entities and individual government authorities, Kazakhstan has demonstrated that even before making these amendments, TFS in accordance with the UN sanction lists were also applied without delay. At the same time, there is a deficiency in the lack of obligation in the AML/CFT legislation to apply TF-related TFS by all natural and legal persons (except obliged entities). The current legislation also does not provide for any specific penalties for natural and legal persons who breach the TFS requirements. The expert assessors note that Kazakhstan, as part of the UNSCR 1373 implementation, has sent requests for mutual freezing only to the EAG member states. Besides that, Kazakhstan has not added any individuals or entities to the international UN lists. Kazakh competent authorities carry out activities aimed at increasing the obliged entities' understanding of obligations to apply TF-related TFS. At the same time, the expert-assessors note that there are certain deficiencies with regard to the identification of customers' BO, which may reduce the effectiveness of the measures applied.

685. Kazakhstan carries out certain work to control NPOs in order to prevent their misuse for TF purposes without prejudice to their legitimate activities, while the work is generally built on the basis of the NRA and TF SRA findings in terms of the misuse of NPOs.

686. In their work with charitable and religious organizations, whose possible misuse for TF purposes is assigned a medium risk level, the competent authorities focus on ensuring the transparency of fundraising and accounting for incoming donations without proper control over the intended use of the financial assistance provided.

687. NPOs sufficiently understand the vulnerability of organizations to the misuse for TF purposes, but there is a need for better mechanisms to inform NPOs of their own actions in the event of relevant threats.

688. Kazakhstan seeks to deprive terrorists, terrorist organizations and terrorist financiers of their assets and instrumentalities of crime by using various methods, including designation, freezing of funds and confiscation as part of TF investigations and proceedings.

689. The measures taken by the authorities of the Kazakhstan are generally consistent with the overall TF risk profile of the country.

690. **Kazakhstan is rated as having a substantial level of effectiveness for IO.10.**

4.4. Immediate Outcome 11 (PF financial sanctions)

691. In 2021, Kazakhstan conducted an assessment of its PF risks, threats and vulnerabilities, although this is not currently required by the FATF Standards. This assessment contributed to the authorities' understanding of risks and exposure of the financial system to PF-related activities.

692. Kazakhstan has no common borders with the DPRK and Iran. Despite the existence of diplomatic relations, there is no embassy of the DPRK in Kazakhstan. There is no trade turnover with the DPRK. The trade turnover with Iran is about USD 300 million in monetary terms (mainly agricultural products, medical equipment, metals, car parts, and timber). There are no Iranian banks or banks with Iranian participation in the country. At the same time, the FMA regularly receives STRs on transactions of Iranian nationals who are clients of the obliged entities and tax residents of the Kazakhstan.

693. Kazakhstan has a significant sector producing goods and materials that could potentially be used for the proliferation of weapons of mass destruction (WMD). Kazakhstan has the world's second-largest uranium reserves and the first-largest uranium production[28]. Although beyond the scope of this assessment, Kazakhstan has an effective customs and export control regime for trade in relevant goods that ensures compliance with the UN sanctions, and applies control measures to financial transactions that may be tied to WMD proliferation Besides that, Kazakhstan has established the WMD Non-Proliferation Interagency Commission under the President of the Kazakhstan. Heads/representatives of MISD, ME, SRC, NSC, MoD and MFA take part in the meetings of the Commission.

694. The combination of the above contextual factors, as well as the measures applied by the national competent authorities aimed at WMD non-proliferation, allow for the conclusion that there are no objective prerequisites for the use of the territory of Kazakhstan for PF purposes.

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

695. The available mechanisms of applying PF-related TFS are similar to those described above in IO.10 and which are related to the regime of application of TF-related TFS. In 2020-2022, Kazakhstan amended the legislative acts of the Republic to improve the mechanism of TFS implementation in terms of compliance with the "without delay" principle. Regulations on TFS implementation procedures were adopted just before the on-site mission. At the same time, Kazakhstan has been generally using the proper system for the application of PF-related TFS in the past few years.

696. The FMA is the competent authority responsible for the formation and maintenance of all sections of the list, including the PF-related section, as well as its dissemination to government authorities, supervisory authorities and obliged entities. At the time of the on-site mission, 239 individuals and entities (80 individuals and 75 entities with regard to the DPRK, and 23 individuals and 61 entities with regard to Iran) were on the PF-related section of the list. The FMA (i) makes the list available to the public on its official website [29]; (ii) notifies the obliged entities through personal accounts; (iii) sends notifications to the obliged entities' email addresses; and (iv) sends notifications to the obliged entities via messengers. In addition, a "Web-SFM" portal has been launched at FMA since 2022 to increase the efficiency of interaction with the obliged entities, including through the TFS.

697. Currently, the FMA receives the relevant UNSC lists directly from the official UNSC website and makes them publicly available on its official website in a fully automatic mode, including on weekends and public holidays, by organising duty rosters of responsible officers in accordance with a schedule approved by the First Deputy Head of FMA (Order 6 dated 29.01.2016 and Order 5 dated 21.06.2021). Until 2020, the FMA received notifications of amendments to the UN sanction lists on the website of the relevant UN Committees by subscription and published them on its website. The PF-related information (similar to the TF-related UN sanction lists) received through the MFA channels is used as an additional source to verify the amendments already made to the list and application of TFS.

698. The time taken by the Kazakhstan to publish updates to PF-related UN sanction lists is provided in Table 11.1.

699. The publication of the lists is the legal basis for the obliged entities to apply measures for freezing the funds and other assets of the persons designated in the relevant UN sanction lists within no more than 24 hours, as well as for the incurrence of liability for violation of these requirements. Despite the time limits specified in the law, in practice this requirement is implemented in less time.

700. On average, Kazakhstan publishes the UN sanction lists on its official website within a few hours. In practice, in most cases, it takes no more than 30 minutes to publish the lists (additions, amendments or removals.

[28] 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

[29] List of entities and individuals associated with the financing of proliferation of weapons of mass destruction https://afmrk.gov.kz/ru/the-list-of-organizations-and-individuals-associa/perechen-organizaczij-i-licz-svyazannyix.html

Table 11.1. Publication by the Kazakhstan of the UN sanction lists (in accordance with UNSCR 1718/2231)

Date of making amendments to the UNSC list	UNSC decision	Publication on the FMA website	Time for publication (days)
14.09.2022	2 entries were amended (1718)	15.09.2022	≤1
26.07.2022	44 entries were amended (1718)	27.07.2022	≤1
30.06.2022	1 entry was amended (1718)	01.07.2022	≤1
11.05.2020	1 entry was amended (1718)	12.05.2020	≤1
08.08.2018	1 entry was amended (1718)	09.08.2018	≤1
09.07.2018	2 entries were amended (1718)	10.07.2018	≤1
23.05.2018	1 entry was amended (1718)	24.05.2018	≤1
30.03.2018	22 entries were amended (1718)	31.03.2018	≤1
15.02.2018	1 entry was amended (1718)	16.02.2018	≤1
22.12.2017	17 entries were added (1718)	23.12.2017	≤1
11.09.2017	4 entries were added (1718)	12.09.2017	≤1
05.08.2017	13 entries were added and 2 entries were amended (1718)	06.08.2017	≤1
05.06.2017	2 entries were amended (1718)	06.06.2017	≤1

701. Order No. 274 provides for the procedures and grounds for de-listing persons, appealing designation decisions (by filing a written application to the FMA, and in case of refusal – by reference to the court) and providing access to frozen assets. At the same time, the FMA has developed and published on its official website a reminder[30] for designated persons, describing in detail the procedure for requesting to de-list or fully (or partially) revoke the applied measures for freezing funds or other property.

702. In the Kazakhstan, under the leadership of the Ministry of Foreign Affairs, an interagency policy is being implemented to consider designation of individuals and entities in accordance with UNSC Resolutions 1718 (with regard to the DPRK) and 1737/2231 (with regard to Iran) and their successor resolutions. Order No. 1009/dsp, which was reviewed by the assessment team during the on-site mission, establishes the procedure for interaction between the relevant authorities before the MFA submits a proposal for designation to the relevant UN Committee.

703. Despite the fact that the procedure for sending proposals to the UN for designation in the PF-related UN sanction lists is statutory and understandable to representatives of the authorities with whom the assessors met, it has not been applied in practice - Kazakhstan has not proposed any individual or entity for designation in the UNSC sanction lists.

704. According to the R.7 analysis, the obligation to apply PF-related TFS does not apply to all natural and legal persons, but only to the obliged entities, since there are no provisions in the legislation of Kazakhstan directly stipulating liability for violation by all natural and legal persons (except FIs, DNFBPs and VASPs) of the prohibition to provide funds and other assets to designated persons. Besides that, in terms of effectiveness, there have been no cases in Kazakhstan that demonstrate the possibility of imposing sanctions on a natural or legal person who has violated the TFS application requirements under UNSCR 1781 or 2231.

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

705. Since 2020, the obliged entities are required to: (i) check the parties to a transaction against the list; (ii) suspend transactions without delay and without prior notice, except for transactions that deposit funds into the accounts of natural persons or entities; (iii) freeze funds or other assets of designated persons; and (iv) send STRs to the FMA if there is suspicion or in case of TFS application.

706. No funds or other assets of natural persons or entities designated in the PF-related list were identified

[30] https://afmrk.gov.kz/assets/files/departament/779-t9gl1c.pdf

in the Kazakhstan in the assessed period.

707. As noted in IO.6, the obliged entities may classify suspicious transaction reports and transactions subject to mandatory monitoring and assign an appropriate code to such transactions. In 2020, the FMA introduced a classification code for PF-related TFS, indicating possible evasion or avoidance of appropriate sanctions. However, as of September 2022, none of the obliged entities had sent STRs with these codes. At the same time, it should be noted that the FMA analyzes information and STRs received from the obliged entities related to the FATF's call for action.

708. As an additional measure in case of suspected PF, Kazakhstan has a mechanism of administrative freezing of assets for up to 16 days (freezing for 15+1 days) in accordance with the FMA's decision. This measure can be applied when there are suspicions that a transaction may be related to an individual or entity designated for PF. However, this mechanism has not been invoked in connection with application of PF-related TFS.

709. With respect to the non-proliferation system as a whole, the SRC analyzes all cross-border transactions in connection with the movement of goods across the customs border and may apply the freezing measures administratively for an unlimited period of time. As of September 2022, the SRC has not invoked this mechanism.

710. Besides that, the NSC, together with the SRC and other authorized bodies, conducts police intelligence activities aimed at controlling the movement of nuclear materials and dual-use goods. For example, during a joint operation by the NSC and the State Security Service of the Republic of Uzbekistan (SSS), a nuclear material supply channel was suppressed (Case Study 11.1).

Case Study 11.1 (Suppression of a nuclear material supply channel)

On the basis of intelligence and operational information, NSC obtained data on Kazakh national A. who intended to sell nuclear material "Uranium-235, 238" in Almaty. During the "control purchase" operation in March 2021, individual A. was detained while attempting to sell 370 grams of "Uranium-235, 238" for USD 200 thousand. During the investigation against individual A., he confessed to his ties in Uzbekistan.

Based on the information received, a decision was made to establish an international investigation team of the NSC and SSS and to conduct a joint operation. In April 2021, five Uzbek nationals and one Tajik national were detained during a controlled attempt to sell 860 grams of nuclear material stolen from the deposit.

In September 2021, the Almaty District Court in Almaty sentenced individual A. to imprisonment for a term of 2 years for offences covered by Article 283(2) and RU CC Article 286. In Uzbekistan, the court also sentenced the other participants in the case to imprisonment for a term of 6 years for offences covered by RU CC Article 252.

The FMA together with the FIU of the Republic of Uzbekistan conducted a parallel financial investigation to establish the facts of involvement of the suspects in PF. However, no such facts were identified.

4.4.3. FIs, DNFBPs and VASPs' understanding of and compliance with obligations

711. As noted in IO.10 and IO.4, the obliged entities have generally demonstrated a good understanding of their obligations to implement TFS enforcement measures. Larger obliged entities have effective sanctions enforcement controls, including automated reconciliation with the PF-related list and commercial databases. All of the obliged entities have access to a personal account on the FMA official website through which they receive updated lists. Smaller obliged entities, on the other hand, have less sophisticated controls and have to check their client databases manually.

712. All FIs and DNFBPs with whom the assessment team met during the on-site mission were aware of

their obligations to apply PF-related TFS, including the possibility of suspending a transaction and sending an STR to the FMA for financial analysis to confirm or deny suspicions. Besides that, the obliged entities were aware of their obligations to screen new customers prior to accepting for service to see if they were designated.

713. In the Kazakhstan, the requirements for the application of PF-related TFS also apply to VA. VASPs registered in the AIFC and not registered in the AIFC are required to comply with all AML/CFT legislation requirements, including CPF measures. At the time of the on-site mission, however, 8 VASPs were operating in the AIFC, of which 2 were active. Transactions conducted through them are very limited. At the same time, there were no VASPs not registered in the AIFC at the time of the on-site mission. Kazakhstan has not yet implemented the freezing of VA on PF-related grounds.

714. One of the prerequisites to effective implementation of PF-related TFS is whether FIs, DNFBPs and VASPs correctly identify the customer's ultimate BO or transaction parties. As the expert assessors were able to verify during the on-site mission, the obliged entities understand their obligations to identify the customer's BO. However, there are some deficiencies in identifying customer's BO (see IO.4) that may reduce the effectiveness of the measures applied. At the same time, this is mitigated by the fact that the obliged entities do not use a formal approach to BO identification. The information provided in the frame of CDD directly by the customers is verified using various commercial databases. If there is any doubt as to whether the person with the controlling interest is the BO, the obliged entities confirm this information during the analysis of the customer's transactions. In some sectors, the obliged entities have recorded cases of refusal to establish a business relationship when the ultimate BO cannot be identified.

4.4.4. Competent authorities ensuring and monitoring compliance

715. During the on-site mission, the expert assessors were convinced that the competent authorities of the Kazakhstan monitor and to a large extent ensure the compliance of the obliged entities with their obligations to apply PF-related TFS. The country has demonstrated effective approaches to informing the private sector on the AML/CFT/CPF requirements and related risks.

716. The ARDFM, FMA and AFSA on a regular basis inspect their obliged entities for compliance with the requirements for the application of PF-related TFS, and no facts of violation of the relevant obligations have been identified.

717. In addition to publishing and disseminating the list of PF-related TFS, the FMA also publishes additional information on the application of PF-related TFS on its official website and in personal accounts. For example, in 2020 and 2022, the FMA sent guidance to the government authorities and obliged entities on the implementation of TFS and submission of STRs associated with the possible avoidance of PF-related TFS. Besides that, in 2021, the FMA developed and disseminated PF typologies to the obliged entities. In February and March 2022, FMA held training events for obliged entities to raise their awareness of the requirements of the RK legislation in relation to the application of PF TFS. The FMA website also contains memos for the obliged entities, which include information on PF-related TFS requirements.

718. However, the expert assessors believe that the obliged entities' awareness of their obligations to apply PF-related TFS can be improved by developing and disseminating more detailed guidelines on the practical application of PF-related TFS.

719. Most obliged entities in meetings with the assessment team noted that they contact the FMA on a regular basis and receive clarifications on legal requirements and the practical application of PF-related TFS via messengers and newsletters in a timely manner.

Overall conclusion on IO.11

720. Given that the Kazakhstan has taken practical measures to ensure designation of persons involved in PF in the list without delay, its dissemination to the obliged entities and application of freezing measures, the country has demonstrated a significant level of effectiveness. The existing practical mechanisms of implementation of PF-related TFS are the same as those established by the UN for TF-related TFS. The

expert assessors note the need for modest improvements related to establishing liability for individuals and entities (that are not obliged entities) who violate the obligation to apply PF-related TFS; developing more detailed guidelines for the obliged entities on the practical TFS application; and detecting and identifying entities owned by or associated with the persons designated for PF.

721. **Kazakhstan is rated as having a substantial level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

Financial institutions

1. All obliged entities, except for commodity exchanges, have good knowledge and understanding of their AML/CFT obligations and risks existing in the country, their sectors and institutions. The obliged entities have a good understanding of the ML risks, and at lesser extent FT risks.

2. At the same time, based on the NRA most obliged entities, except for STBs and certain PSP and insurance companies, consider vulnerabilities of involvement in predicate offences as ML/TF risks, but believe that they do not face risks of being involved in ML/TF schemes.

3. In most obliged entities the internal control measures are based on the statutory requirements set out in the legislation. At the same time, certain obliged entities (this mostly concerns STBs and PSPs and insurance companies) demonstrated implementation of their own internal risk mitigation measures.

4. All obliged entities apply CDD measures to customers and their beneficial owners and verity data using open and commercial databases and information sources. At the same time, some non-banking FIs tend to rely on the internal controls exercised by the STBs when opening and maintaining a customer's bank account or conducting transactions, which reduces the effectiveness of CDD measures in the view of the Assessment team.

5. Some of the obliged entities, irrespective of a sector, identify individuals owning, directly or indirectly, 25 or more percent of shares of legal entities as BOs without verifying whether or not actual control of a legal entity is exercised through other means.

6. All obliged entities assign risk ratings to their customers based on the criteria set out in the legislation and Internal Control Rules. The practice of applying regular, simplified and enhanced CDD measures varies across sectors and also individual obliged entities. A different set of CDD measures, depending on the risk level assigned to the client, is applied mainly in STBs, and to a lesser extent in other sectors.

7. In general, the obliged entities apply enhanced CDD measures when establishing business relationships with higher risk customers, including PEPs, if any. At the same time, the practice of some obliged entities shows that for the existing customers, the assigned risk ratings seem to have little effect on intensity of applied CDD measures, but determine primarily the frequency of customer updates and enhanced monitoring of transactions. Some individual obliged entities refuse or terminate business relationships with high-risk customers.

8. Obliged entities apply targeted financial sanctions, deny transactions, refuse to establish and maintain business relationships, and freeze assets.

9. In general, the obliged entities are reasonably well aware of and fulfils their obligations to send STRs regarding proceeds of crime and, to a lesser extent, terrorist financing. The bulk of STRs are sent by the STBs, that is in line with the risk profile of Kazakhstan. At the same time, some obliged entities (commodity exchanges and insurance brokers) did not send or sent relatively few STRs, that cannot be explained by their low risk profile alone and is indicative of a lack of understanding and compliance with the STR reporting obligation.

10. Failure to send or late sending of STRs is one of the most frequently detected violations of AML/CFT legislation.

DNFBPs and VASPs

11. The AML/CFT legislation applies to all categories of DNFBPs and VASPs existing in the country. DNFBP sectors, except for lawyers, and VASPs demonstrates a good level of understanding of their AML/CFT obligations. Understanding of AML/CFT obligations by the lawyers is limited due to the fact that only a small portion of their professional activities is subject to the AML/CFT Law.

12. DNFBPs and VASPs have demonstrated a good understanding of threats, vulnerabilities and country risks as a whole. However, no separate ML/TF risk assessments have been conducted in the DNFBP sectors, which may have a negative effect on the level of understanding of risk present in these sectors.

13. DNFBPs and VASPs take measures to mitigate ML/TF risks by applying enhanced CDD measures and conducting monitoring of transactions taking into account the specificities of their activities. When transactions meet the suspicious criteria and indicators, DNFBPs and VASPs report such transactions to the FMA.

14. There are some shortcomings in identification of BOs of those parties to transactions who are natural persons. This particularly applies to those categories of DNFBPs that provide services to natural persons (real estate agents, bookmaker offices) and VASPs.

15. There is a limited understanding of how to identify domestic PEPs, as this requirement has been implemented into the AML/CFT Law quite recently, and a good understanding of the application of TFS and the identification of customers from high-risk countries. DNFBPs apply group internal control policies to the extent not contrary to Kazakhstan legislation.

16. DNFBPs and VASPs have a good understanding and practical implementation of the CDD and record keeping procedures. Not all DNFBPs report a refusal to establish a business relationship.

Recommended Actions

Financial institutions

1. When assessing internal risks, all obliged entities should take into account risks of their potential involvement in ML/TF schemes and apply adequate risk mitigation measures correlating to the specificities of their activities.

2. When identifying BOs of legal persons, the obliged entities should not only identify ownership of 25 per cent or more of the share capital, but also identify BOs exercising effective control over the legal person. To this end, it is recommended to expand measures to verify the details of the BO of resident customers, including but not limited to the use of available public or commercial databases.

3. The obliged entities should apply enhanced CDD measures in respect of higher risk customers and not refuse to establish business relationships with such customers, where appropriate.

4. Non-bank obliged entities should improve their risk-based approach to CDD and more systematically apply regular and simplified and enhanced CDD measures appropriate to the risk level of clients, and tailor the intensity and scope of such measures to the specific circumstances of clients, in addition to the frequency of clients updates.

5. Commodity exchanges and insurance brokers should improve understanding of their obligations related to reporting and identification of suspicious transactions.

6. Non-bank FIs should develop their own suspicious indicators with due consideration for their risk profiles, where appropriate.

7. The decision-making process for recognising a transaction as suspicious should be improved so that the transaction is suspended before it is conducted, where appropriate.

DNFBPs and VASPs

8. For better understanding of sectoral risks, DNFBPs shall conduct regular assessments of individual risk profiles of the clients.

9. DNFBP and VASPs should continue the work on improving guidelines and procedures clarifying the tools of identification of BOs of the individuals, associates with BOs and domestic PEPs.

10. It is recommended the country to maintain the interaction between the MoJ, The Council of Bar Association and the FMA to strengthen lawyers' understanding of their AML/CFT obligations.

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

5.2. Immediate Outcome 4 (Preventive Measures)

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

723. The assessment and conclusion on IO4 is based on interviews with the private sector in Kazakhstan, statistical data and case studies provided by the country.

724. For the purpose of the effectiveness assessment, the important obliged entities include STB, securities market participants, EEMA, postal operator, dealers in precious metals, precious stones and jewelry, real estate agents, organisers of gambling industry. Sectors of insurance (reinsurance) companies, payment service providers, leasing companies, exchange offices run by authorized institutions, notaries, accounting firms and professional accountants, VASPs are identified as moderately important. And the entities engaged in certain types of banking operations, commodity exchanges, lawyers, legal advisors, other legal professionals, audit firms and AIFC members (except for VASPs) were weighted as being of low importance (see para 168-195 of the Report).

Financial institutions

725. FIs (except for commodity exchanges), including the AIFC members, demonstrated a good awareness and understanding of their AML/CFT obligations set out in the AML/CFT Law, other laws and regulations and internal control rules.

726. All FIs have a compliance service or compliance officers responsible for AML/CFT monitoring, clarifying the statutory requirements to personnel, developing and implementing the internal control procedures and interacting with the designated and supervisory authorities on AML/CFT issues, including CDD, record keeping and suspicious transaction reporting.

727. Unlike other FIs, the commodity exchanges show insufficient understanding of their AML/CFT obligations.

728. FIs (except for commodity exchanges) have demonstrated sufficiently good awareness and understanding of their own ML risks and ML risks identified in the NRA, but a weaker understanding of FT risks.

729. All FIs (except for FI in AIFC) were engaged in the NRA exercise by providing information through their professional associations. The NRA findings have been communicated to the FIs that use them for reviewing their internal risks and developing CDD and risk mitigation measures. Based on the interviews and examples provided, the assessors were able to conclude that the FIs (except for commodities exchanges) know and understand their sectoral risks and take into account the ML typologies specific to their sector of operations. Assessors consider that the risk level of FIs is generally consistent with the country's risk profile.

730. At the same time, most interviewed FIs, except for STBs and few of insurance companies and one PSP, considered ML risks as risks of exposure of FI in predicate offences, and believed that they are not exposed to risks of being involved in ML schemes. The assessors consider this approach as acceptable in the context of Kazakhstan (see IO1), but it is recommended FIs to improve their understanding of the risks of involvement in ML schemes in order to comply with the FATF standards.

731. Understanding of own and sectoral FT-related risks is moderate as most FIs, with the exception of STB, are NRA-oriented (see IO1). Understanding relates mainly to the obligation to identify designated persons amongst FIs' customers. STBs, KazPost and PSPs mainly reported TF-related STRs, and other FIs have not sent or have sent very few such STRs, that indicates a moderate understanding of FIs' risks of involvement in TF in the context of Kazakhstan, according to assessors.

732. Unlike other FIs, the commodity exchanges insufficiently understand ML/TF risks associated with their activities. The interviewed commodity exchanges, as well as the APCD, believe that there is practically no ML/TF risk, as no money flows through the commodity exchanges, and trading is conducted with goods, the sale of which is regulated and controlled by the competent authorities on the basis of monthly reporting. Nevertheless, the complete absence of ML/TF risk in the activities of commodity exchanges is not evidenced in the context of Kazakhstan, as the RBA in supervision was at the initial stage as of on-site mission, and the risks of the brokers' customers were not taken into account while assigning risk levels to the traders of commodity exchanges.

733. Most AIFC member companies were not engaged in the NRA exercise, as a large number of them launched their activities quite recently. Nevertheless, some obliged entities operating in the AIFC develop the internal AML/CFT procedures with due consideration for the vulnerabilities of potential misuse of legal entities identified in the NRA. Also, interviews conducted with FIs in AIFC allow to conclude that they have a good understanding of their own ML/TF risks and that the level of risk assigned is consistent with the AIFC risk profile.

DNFBPs and VASPs

734. Representatives of all categories of DNFBPs noted that the NRA exercise was very useful and helped them to better understand their AML/CFT obligations and ML/TF risks. All DNFBPs understand their AML|CTF obligations. Notaries, legal professionals, real estate agents and dealers in precious metals and stones have demonstrated most comprehensive understanding of their obligations.

735. All DNFBPs have a good understanding of ML risks, while the level of their understanding of TF/PF risks is somewhat lower. Risk understanding has been developed through participation of all categories of DNFBPs in the NRA exercise as well as through training provided by the FMA and sectoral SRBs.

736. The NRA coverage was quite extensive, and such sectors as audit firms, organisers of gambling industry and AIFC members, including VASPs, were fully involved in the risk assessment. The sectoral SRBs also proactively contributed to the NRA process by disseminating questionnaires to the obliged entities and collecting and analyzing the received responses.

737. All interviewed DNFBPs demonstrated a good understanding of threats and vulnerabilities identified in the NRA and risks existing in their sectors. DNFBP representatives reported that criminal proceeds are laundered through underground casinos, real estate property, jewelry and other high-value goods. Criminal proceeds are generated by fraud scams and Ponzi schemes, investing dirty money into illegal business activities, committing tax crimes and using fake/ false documents. These are in line with NRA-2021 results.

738. All categories of DNFBPs have shown a good understanding of risks of misuse of their sector for illegal activities. Among them, the best understanding of risks of potential misuse of services for illegal purposes has been demonstrated by accountants, legal advisors, jewelers and organisers of gambling industry.

739. All DNFBPs understand their relevant sectoral risks and develop internal control rules with due consideration for the identified threats and vulnerabilities. In practice, the major ML/TF risks and risk-typologies are taken into account by DNFBPs (except for lawyers) in practice taking into account the specificities of their activities. However, the lawyers, along with the legal assistance guaranteed by the State, also render a comprehensive social legal assistance services by way of providing a legal support to clients since their official application for legal assistance through resolution of a case, i.e. their activity is not limited to representation of clients in court. Socially vulnerable groups (e.g. retired persons, war

veterans, elderly and disabled people residing in assisted-care facilities) are eligible to receive such assistance.

740. VASPs are subject to the AML/CFT obligations. VASPs have demonstrated a good awareness and understanding of AML/CTF obligations and ML/TF risk mitigation measures, that undoubtedly influenced by the sector assessment, and evidenced by the reporting examples and statistics that have filed not just threshold reports, but also suspicious transactions reports and also refused to establish and terminated business relationships with customers. Most reports are related to suspicious transactions: in 2021, of total number of filed reports, 77% were suspicious transaction reports, 14% were threshold transaction reports and 9% were other reports, while in 2022, 84% were suspicious transaction reports, 7% were threshold transaction reports and 9% were other reports.

741. VASPs have a good understanding of ML/TF risks associated with the use of digital assets. The AFSA has conducted assessment of ML/TF associated with digital assets, and all stakeholders have agreed with the conclusion that digital assets pose high vulnerability due to their anonymity. In this context, the certain measures have been applied to mitigate risks of misuse of digital assets for criminal purposes, *inter alia*, for terrorist activities. In particular, operation of P2P platforms is prohibited, non-identified transactions are denied, and maximum transaction amount is limited to USD 100 or 1 BTC for natural persons and to 3 BTC for legal entities, and the use of digital assets is prohibited to conceal the movement of funds on blockchain networks and only licensed VASPs are allowed to interact.

5.2.2. Application of risk mitigation measures

Financial institutions

742. In general, the FIs have demonstrated the mechanisms in place for mitigation customer risks, transactional risks, geographic risks and delivery channel risks.

743. Despite the declared individual approach to internal assessment of risks, the provided examples show that most FIs use the rule-based approach and implement ML/TF risk management measures based solely on the legislative and regulatory requirements to the Internal control rules (IRC) adopted by the supervisors in consultation with the FMA (suspicious transaction indicators, typologies, risk-based approach, transaction thresholds, training and reporting), and do not consider specific individual risk factors associated with customer base risks, product risks, etc. Also, most non-bank FIs consider not providing financial services without opening a bank account and not using cash as the main risk mitigation measure.

744. At the same time, certain FIs demonstrated that they include their own risk reduction mechanisms in the IRC, such as limited value and volume of the most vulnerable transactions (second-tier banks, payment service providers), enhanced due diligence of counterparties (PSPs), prohibition of omnibus accounts (securities market participants), development of their own suspicious transaction indicators (STBs, PSPs, insurance companies), engagement of compliance service in development and ML/TF risk assessment of new products (insurance companies), automated risk rating assignment and transaction reporting procedures, etc.

745. When establishing business relationships, all FIs determine customer risks in line with the requirements set out in the legislation and internal control rules. However, some EEMAs and commodity exchanges assign customer risk ratings not related to ML/TF, but associated with other factors as insolvency. Besides that, some obliged entities apply a rule-based approach to determine customer risks and assign only two degrees of risk (low and high) to customers as required by their internal control rules.

746. Most obliged entities use the automated procedures for assessing and determining risk level. Customer risks are reviewed and re-assessed periodically, depending on level of risk originally assigned to a customer and also in certain situations (identification of suspicious transaction, inclusion of a customer in the sanction lists, etc.). However, the assessors were provided with a limited number of examples when the degree of risk assigned to the existing customers was reviewed in practice - it has been done primarily after designation and inclusion of banks' customers in the sanction lists. One PSP presented the example

when it increased the degree of risk assigned to one of its customers. Another example was provided by a securities market participant when it reduced the degree of risk originally assigned to its customer after the country of location of this customer was deleted from the list of offshore territories.

747. The FIs in AIFC effectively apply measures for mitigating risks associated with their activities in line with the AIFC context and requirements of the internal control rules and other AIFC internal regulations. Measures aimed at mitigation of risks identified in the country are applied to a limited extent as the FIs in AIFC do not consider these risks as significant for their sector.

748. During the interviews certain obliged entities informed that they refused to establish or maintain business relationships with high risk and non-resident customers with a view to mitigating ML/TF risks. In case of certain obliged entities, such approach (for instance remote establishing of business relationships) is driven by their business models as well. The supervisory authorities are well aware of such practice and conduct awareness-raising activities to prevent unjustified refusals to establish business relationships.

DNFBPs and VASPs

749. In order to identify the risk of their clients the real estate agents, dealers in precious metals and stones, organisers of gambling industry, legal advisors, notaries and audit firms divide them into three groups (high, average and low risk), while accountants and lawyers employ a two-levels of risk (high and low). However, lawyers reported that based on practice they do not perform activities (transactions) covered by the AML/CFT Law.

750. If a customer does not fall into a low risk category, DNFBPs apply enhanced due diligence and monitoring measures in respect of such customer. They carefully scrutinize transactions of such customers and (or) repeatedly request them to provide documents or information about their business activities and origin of funds and (or) seek a senior management approval for maintaining business relationships with such customers. Dealers in precious metals and stones (jewelers) have demonstrated the most comprehensive understanding of enhanced due diligence and monitoring measures.

751. If the highest degree of risk is assigned to a customer (typically in case of inclusion of a customer in the lists of entities and individuals linked terrorist and extremist activities, TF ad PF, or if a customer is the resident of a country that does not comply with the FATF Recommendations), DNFBPs will refuse to establish or maintain business relationships with such customer. However, there were no cases of refusals in the practice of DNFBPs at the time of the on-site mission.

752. Accountants, real estate agents, legal advisors, jewelers update the data of their high-risk clients at least once a year.

753. With a view to mitigating risks, almost all DNFBPs have implemented the automated procedures, including internal control procedures, and some categories of DNFBPs (e.g. notaries) have developed special software that includes AML/CFT elements (monitoring of customers and transactions, screening against sanction lists). The degree of automation is less extensive in certain entities operating in the real estate sector, but it does not seem to have a negative impact of the effectiveness of application of internal controls so far.

754. VASPs apply risk mitigation measures based on the requirements set out in the internal control rules and other AIFC internal regulations.

755. In the course of application of risk mitigation mechanisms, VASPs in AIFC analyze customers in terms of their types (profiles) and service delivery channels (only remotely), and also consider geographic risk factors and risks associated with IT products used by customers (digital assets, VASP wallets, cold wallets, links to suspicious and sanctioned wallets). After that, customers are classified under three risk categories (medium, medium high and critically high).

756. In case of a medium risk of client, VASPs update the client's details at least once a year and where the risk level is higher, the business relationship can be terminated. Should the level of risk is critically

high, VASP in AIFC shall refuse to establish a business relationship and inform both FMA and AFSA.

757. With a view to mitigating risks, VASPs maintain "black" lists of customers. For example, termination of business relationships constitutes the grounds for inclusion in this list, while designation of a customer as an individual or entity linked to terrorism and extremism, TF and PF or residency/ location of a customer in a country that does not comply with the established requirements constitute the grounds for termination of business relationships. Besides that, VASPs cross-check each wallet transaction against the lists (sanctions, mixers, Darknet, etc.) using the blockchain analytic tools.

5.2.3. Application of CDD and record-keeping requirements

Financial Institutions

758. In general, FIs effectively comply with and apply CDD measures, identify customers and verify customer data when establishing business relationships, review and update information on existing customers on a regular basis, and conduct monitoring of transactions. However, there are certain shortcomings related to identification and verification of BOs of customers.

759. FIs identify customers and further verify customer data against the state databases of natural persons and legal entities using individual and business identification numbers. Non-resident customers are identified by way of collecting ID documents or constituent documents and their data are verified against commercial databases and publicly accessible information sources. Thus, Kazakhstan residents are subject to full and accurate identification, while non-residents are verified using reasonable measures available to obliged entities.

760. FIs identify and verify BOs of resident customers by way of gathering information from documents and questionnaires provided by customers (charters, registers, state registration certificates) and from the government databases and the stock exchange database. BOs of non-resident customers are identified and verified using publicly accessible sources and commercial databases.

Case Study 4.1 (Kaspi Bank)

In 2021, a legal entity (limited liability company) applied to the Bank for opening a bank account. Using the publicly accessible information sources, the Bank identified the beneficial owner of this company as the designated person included in the list of terrorists by a foreign country and refused to establish business relationships.

761. At the same time, the provided BO identification examples show that FIs often identify individuals owning, directly or indirectly, 25 or more percent of shares of legal entities as BO without verifying whether or not control of a legal entity is exercised through other means.

762. FIs that provide services only to natural persons (EEMA, AIs) do not identify BOs, but instead verify whether or not customer personal data or false/forged documents are illegally used for receiving services by third parties.

763. Certain FIs (STBs, AIFC members) refuse to establish business relationships when potential customers fail to provide documents necessary for conducting CDD, *inter alia*, for identifying BO. However, in most cases, obliged entities refuse to establish or maintain business relationships due to other reasons (sanction list positive match, ML/TF suspicion, etc.).

Table 4.1. Number of Business Relationship Denial STRs

	2018	2019	2020	2021	2022
STBs	3100	3491	*138*	*3 626*	*3 836*
Insurance (reinsurance) companies			*5*		
Commodity Exchanges	1	1		*1*	
Microfinance organizations		5		*6*	
Payment service providers	1				*4*
Notaries		1		*1*	

AIFC members				*16*	*13*
Securities market participants		1			
Post operator		37			

764. Most FIs conduct CDD themselves using their own resources. However, the interviewed non-banking FIs explained that they rely to a certain extent on the internal control, exercised by STBs when opening and maintaining the customer's bank accounts or conducting transactions, as the services of such FIs are performed through the customer's bank account, and this is confirmed by the NRA report (NRA Report on ML). This approach is assessed as having a negative impact on the effectiveness of CDD measures.

765. In some cases, PSPs and insurance companies rely on CDD conducted by insurance agents, counterparties or a holding company. In doing this, PSPs and insurance companies verify compliance by a third party on which they rely with the AML/CFT requirements and repeatedly cross-check positive matches against the sanction and PEP lists.

766. However, some non-bank obliged entities rely on internal controls performed by the STB while opening and maintaining the customer's bank account and conducting the transaction, when implementing CDD measures, as mentioned in the NRA report (NRA Report on ML).

767. There is no common approach among FIs to application of simplified, regular and enhanced CDD measures in the process of establishing business relationships. Regardless of a sector, some FIs apply only enhanced (in respect of high risk customers, if any) or simplified (in respect of medium and low risk customers) CDD measures, but do not use regular measures. Other obliged entities do not use simplified CDD measures, but apply only enhanced and regular measures, *inter alia*, in respect of low risk customers.

768. In all FIs, except for STBs, the risk ratings, assigned for the existing customers, determine primarily the customer information reviewing and updating frequency. The information updating frequency is set out in the internal control rules – typically, in case of high risk customers, information is updated at least once a year, in case of medium risk customers – once in 2-3 years, and in case of low risk customers – once in 3-5 years. The level of customer risk in a STBs affects the extent of CDD measures, including measures to examine and analyse customer transactions, the application of enhanced internal control procedures for AML/CFT purposes (re-identifying the customer with a direct contact with the bank), requesting additional documents and analysing them, setting limits on a particular type of transaction.

769. FIs understand the record-keeping obligations and take all available measures for retaining documents, records and information collected in the process of conducting CDD, carrying out transactions and maintaining business relationships for at least 5 years following completion of a transaction or termination of business relationships. No exemptions from this rule have been identified, and no breaches of these obligations have been detected by the supervisors. Although statistics on requests of competent authorities for information from the FIs are not available, according to information provided by the supervisory bodies in practice FIs have always been able to provide necessary information at request of the supervisory or law enforcement authorities. According to the information provided by FIs, electronic customer files are typically kept for indefinite period of time.

DNFBPs and VASPs

770. In general, DNFBPs have demonstrated a good understanding of the CDD and record-keeping procedures and their practical application. Real estate agents, organisers of gambling industry, notaries and advocates provide services primarily to natural persons.

771. DNFBPs identify resident customers and further verify customer data using the individual and business identification numbers. Bookmaker offices use biometric identification when identifying customers through systems integrated with the State database “Natural Persons”. Non-resident customers are identified by way of collecting data from ID documents or constituent documents and their data are verified against commercial databases and publicly accessible information sources. In the course of identification and verification of customers, certain DNFBPs (real estate agents, dealers in precious metals and stones, legal advisors, accountants) communicated that they also rely on the lists of individuals and

entities linked to terrorism, extremism, TF and PF and the list of countries that do not comply with the FATF requirements posted in Personal Accounts on the FMA website as well as lists of sources recommended for CDD and at-risk individuals associated with fictitious invoicing. When identifying and verifying gambling participants, organisers of gambling industry also use the list of persons restricted from gambling and betting maintained by the MCS. The presence of a persons on such a list means that they are prohibited from gambling and betting.

772. DNFBPs have a good understanding of the BO-related requirements. However, organisers of gambling industry, notaries and real estate agents consider that BOs of customers who a natural persons are the customers themselves and do not take measures to identify and record data on BOs of such customers. Meanwhile, real estate agents identify nominal owners of property acting in the interests of third parties. Lawyers provide services to represent the interests of individual clients themselves given the specifics of their work in Kazakhstan.

773. DNFBPs collect information about BOs of their customers through the use of questionnaires. These questionnaires are completed by DNFBPs themselves based on information provided by customers. Information about BOs of non-resident customers is verified by using publicly accessible and commercial databases.

774. Besides that, those categories of DNFBPs that frequently carry out one-off transactions and provide services to occasional customers (notaries, real estate agents, casinos) have also demonstrated the use of customer' psychological profiles (e.g. attempts to avoid identification, analysis of customer behavior, etc.).

775. Other categories of DNFBPs (accountants, legal advisors) have demonstrated understanding and practical application of CDD measures, including such elements as verification of BO information against different publicly available sources or databases accessible for a nominal fee. The Chamber of Notaries has developed and implemented a Single Automated Notary Information System, in which the state databases "Legal persons" and "Natural persons" are integrated. Those databases are used for identification and verification of customers by notaries. In cases where a Kazakh audit firm is a member of an international audit network, audit firms have the opportunity to use the internal rules of that network to request information, including information on the BOs of a representative office (branch) of a foreign company audited in Kazakhstan.

776. DNFBPs are aware of the obligation to refuse to establish or terminate business relationships if customers fail to provide information necessary for identification and verification and comply with this obligation in practice. However, not all DNFBPs report such cases to FMA. For example, real estate agents do not complete CDD procedure when they refuse to establish business relationships.

777. The FMA received 28,668 business relationship denial or termination reports (or 0.26% of total number of reports filed with the obliged entities in 2017-2022). Most such reports were filed by second-tier banks - 28 343 reports or 0.25% of total number of reports submitted to the FMA by STBs, while 325 reports (or 0.003% of total number of reports received by the FMA) were filed by other categories of obliged entities, 12 of which were submitted by DNFPBs.

778. Since 2020, information on refusal to establish business relationships is provided to the FMA in forms of STRs.

Table 4.2. Statistics on STRs related to refusals by DNFBPs and VASPs in establishing and termination of business relationships

	2017-November 2020	December 2020	2021	2022
Notaries	3		1	1
Organisers of gambling industry	5		2	
AIFC members – VASPs			16	13

779. There were no instances when organisers of gambling industry, accountants, legal advisors, audit firms, dealers in precious metals and stones and DNFBPs in AIFC refused to establish business

relationships with customers. If, before executing a transaction, a customer fails to provide the ID document to a real estate agent, such customer is denied further services. Lawyers are aware of the CDD obligations. However, in view of the specificities of services provided by lawyers (legal professional privilege), the lawyers representing the sector during the on-site mission had no clients who applied for legal services covered by the AML/CFT Law.

780. DNFBPs have a good understanding of the record-keeping obligations and take all available measures for retaining documents, records and information collected in the process of conducting CDD, including data on BOs, carrying out transactions and maintaining business relationships for at least 5 years following completion of a transaction or termination of business relationships. No exemptions from this rule have been identified.

781. Besides that, certain DNFBPs (notaries, real estate agents, accountants, legal advisors) keep documents and other records in hard copies or electronic form in the archives for more than 5 years and are able to reconstruct individual transactions where necessary. Examples of law enforcement requests from audit organisations and the provision of relevant materials (reports with working papers) drawn up more than 10 years ago have been demonstrated to the assessors.

782. In the course of CDD, VASPs collect and examine information about customers and their beneficial owners through the use of questionnaires. A wide range of data, including various certificates and constituent documents, are provided in the process of completion of a questionnaire. Each customer and beneficial owner is screened against the list of individuals and entities linked to terrorism, extremism, terrorist and proliferation financing, and is checked for residency in countries that do not comply with the FATF Recommendations.

783. With a view to identifying customer beneficial owners, apart from questionnaires, certificates and constituent documents, VASPs also use the register of beneficial owners (maintained by the AFSA) for identifying beneficial owners of their customers and which at the time of the on-site included data on 1,670 beneficial owners.

784. VASPs in AIFC and DNFPBs in AIFC are aware of the obligation to retain documents and keep them. AIFC law prescribes that documents must be kept for at least 6 years from the date of submission of a notice or report, termination of a business relationship or completion of a transaction. All VASPs in AIFC and DNFBPs in AIFC are registered less than 6 years ago..

5.2.4. Application of enhanced CDD measures

Politically exposed persons

785. According to the ML NRA, there is a risk of involvement of PEPs in corruption and tax offences in Kazakhstan.

786. Obliged entities establish and identify foreign PEPs among their customers and their beneficial owners. Commercial databases are the primary source of information about foreign PEPs and PEPs of international organizations. However, since many obliged entities do not establish business relationships with non-residents, there is no common practice of identification of foreign PEPs and application of enhanced CDD measures to them among obliged entities (except for second-tier banks, insurance companies, professional securities market participants and AIFC members).

787. Although the requirements related onboarding and serving domestic PEPs have been established in the legislation relatively recently, all obliged entities are aware of persons falling into the category of domestic PEPs since the list containing the names of the national PEPs, their family members, close associates and PEPs whose public functions expired no more than 12 months ago is posted in the Personal Accounts of obliged entities on the FMA website. To identify PEPs the real estate agents, accountants, legal advisors use data from social networks and internet sources, in addition to the data in the Personal Accounts of the FMA website. It should be noted that some obliged entities have not yet included the domestic PEP identification requirements into their internal control rules. Nevertheless, the STBs and jewelers identified

domestic PEPs before these requirements were established in the legislation, as on their own or if required by the policies of the financial groups they belonged to.

788. FIs have demonstrated a good understanding of PEP-related risks and enhanced CDD measures aimed at mitigation of these risks, such as enhanced monitoring of transactions. For example, leasing company identified a customer closely associated with the PEP and applied for the Board of Directors' approval for establishing business relationships with this customer. Later, the STR regarding this customer was filed with the FMA. One STB refused to establish business relationships with the customer closely associated with the PEP who had negative press.

789. It should be noted that obliged entities other than STBs in the period of analysis have a very limited number of PEP customers or do not have PEPs as customers at all due to, inter alia, lack of recourse.

790. VASPs have a good understanding of the procedures for PEPs and apply measures to identify them. When establishing business relationships, VASPs remotely verify whether each customer falls into the PEP category. Foreign PEPs are identified through the use of commercial databases and questionnaires, while domestic PEPs are identified by crosschecking their personal data against lists posted in the Personal Accounts of the FMA website.

791. The interviewed DNFBPs have no customers who are PEPs and their family members. All of them have demonstrated knowledge of some measures aimed at mitigating PEP-related risks, i.e. customers who are identified as PEPs are treated as posing higher risk and, therefore, are subject to enhanced CDD measures, including the need to obtain a senior management approval for establishing business relationships even in case of occasional transactions.

Correspondent banking

792. STBs maintain no nostro and vostro correspondent accounts and also have no nested and pass-through accounts. Meanwhile, one of the STBs declared the existence of third-party financial institutions' vostro accounts of their subsidiaries located abroad. However, no information was provided on the measures taken to verify these financial institutions.

793. When opening correspondent accounts, STBs conduct due diligence on respondent and correspondent institutions. Where it is impossible to complete such due diligence process, second-tier banks refuse to open accounts. In particular, certain STB refused to open correspondent accounts for foreign banks on several occasions. In the analysed period, no new correspondent accounts have been opened by STBs.

New technologies

794. Most obliged entities use new technologies for conducting CDD, assessing customer risks, selling products and providing services. Technology solutions are provided mainly by third-party developers. Risks associated with new technologies are assessed only if high-tech products are developed by most obliged entities themselves (except for STBs), while reliability of high-tech products developed by third-party suppliers is not tested. There were instances of imposition of sanctions on obliged entities for breaches of the legislation as a result of failure/ malfunction of the software developed by third-party suppliers. For example, in 2018, as a result of malfunction of the automated transaction reporting system of one professional securities market participant, some STRs were not filed with the designated government agency during a whole day. In these situations, the supervisors imposed fines and implemented the supervisory response measures.

Case study 4.2

One major STB uses an "ORAP" procedure to identify and measure operational risk, including risk assessment of business processes and systems, including new technologies, regardless of whether the implementation side of the solution is external or internal.

Another STB performs due diligence of the software developer on compliance with AML/CFT legislation, including risk assessment of the organisation. Before launching the development into

practical use, it is tested for a trial period, and afterwards the development is periodically checked for quality parameters.

795. There are cases of sanctions being imposed on obliged entities for violations of legislation due to technical failures of third-party software. For example, in 2018 there was a failure in the automatic STR dispatch system of one professional securities market participant, and some STRs were not dispatched during the day. Supervisory authorities drew up protocols for imposing fines and took supervisory response measures.

796. Some obliged entities (STBs, AIFC members, securities market participants, bookmaker offices, EEMA, PSP and insurance companies) provide online services to resident customers, which includes remote identification of customers. In Kazakhstan, such method of identification (i.e. remote identification) is considered reliable as customer information is verified and cross-checked against the state databases "Natural persons" and "Legal persons". Obliged entities also apply additional measures, such as biometric identification of customers, for mitigating risks associated with online services.

797. Before launching new technologies and providing high-tech services, DNFBPs assess them in terms of exposure of a specific obliged entity to a risk of being engaged in ML/TF. Factors that increase risks associated with new technologies and high-tech solutions include a possibility of carrying out transactions remotely and CDD outsourcing. If a risk is assessed as too high, DNFBPs refuse to launch a new practice. The best understanding of these issues was demonstrated by organisers of gambling industry and accountants given the specificities of their business.

798. At the time of the on-site visit, there was one "regulatory sandbox" set up in the AIFC with 2 VASPs operating within this regulatory framework. The AFSA has taken in advance a number of regulatory measures to mitigate the risk of misuse of new technologies and high-tech solutions for ML/TF purposes. VASPs deny cryptocurrency transactions that allow anonymity and P2P platforms are banned. The value of transactions carried out through VASPs is limited – the amount of account replenishment and investment is limited to 1 BTC and USD 100 respectively for natural persons, and to 3 BTC for legal entities.

Wire transfers

799. The STBs control the availability of required originator and beneficiary information for wire transfers by using an automatic screening system, which prevents from making incoming and outgoing transfers in the absence of all required information. In practice, there have been no cases of rejection of a transfer due to insufficient details. This is also applicable to transfers made through international money transfer systems. No breaches related to insufficient originator and beneficiary information in wire transfers have been identified by the supervisory authorities. Thus, the control system is assessed as effective.

800. Operating in the AIFC is one member company that may carry out wire transfers, but this company was inactive at the time of the on-site visit. The share of wire transfers carried out through the AIFC member is 0.02% in the total volume of transfers in Kazakhstan. It should be noted that all international wire transfers are carried out by the AIFC member companies through STB.

801. VASPs apply the AIFC rules governing electronic funds transfers. Given that P2P transfers are prohibited by the AIFC and that VASPs outside the AIFC did not exist at the time of the on-site mission in Kazakhstan, technical deficiencies (see criterion 15.9) do not affect the execution of wire transfers, and wire transfers are carried out effectively.

TF targeted financial sanctions

802. The sanction lists of persons (see IO.10 and IO.11) are posted in the publicly accessible section of the FMA website as well as in the Personal Accounts of obliged entities. Notices about changes and updates in the lists are posted on the homepage of the FMA website. Besides that, obliged entities are notified of updates in the lists by e-mail and through messaging apps.

803. Some obliged entities, including VASP in AIFC and some DNFBPs, automatically integrate the lists

into their internal databases and use them when establishing business relationships with customers. Other obliged entities download the lists manually either on a daily basis or upon receipt of notices about updates in the lists.

804. All obliged entities cross-check personal data of customers and their beneficial owners against the lists. Most obliged entities screen customers against the lists automatically, but some obliged entities, primarily with limited number of customers, perform such screening manually.

805. Upon identification of designated/listed person(s) (among both applicants and their BOs) in the course of onboarding process, all obliged entities refuse to establish business relationships and file a relevant report with the FMA (see Tables 4.1 and 4.2).

806. In case of identification of designated/ listed persons among existing customers and their BOs, obliged entities freeze funds of such customers and file a relevant report with the FMA (see Table 4.3).

807. Pursuant to the 2020 amendments in the Law on Postal Service, KazPost is responsible for making settlements and payments necessary for covering basic expenses of all designated/ listed persons at the initiative of STBs. However, frozen accounts of such customers are still kept by STBs and business relationships with them cannot be terminated unilaterally.

808. VASPs and all DNFBPs have demonstrated understanding of the obligations related to application of TFS without delay and prohibition from tipping-off customers about actions taken against them.

809. Real estate agents screen customers against the list of persons linked to TF or PF posted in the Personal Accounts on the FMA website only in the process of identification.

Table 4.3. Number of Matches with TF and PF Sanctions Lists Reported by Obliged Entities

Categories of Obliged Entities	2018	2019	2020	2021	2022
STBs	1,779	1,039	1,297	1,103	465
Central depository	2	17	6		3
Securities market participants	1			6	
Entities engaged in certain types of banking operations			1		
Commodity exchanges					1
KazPost	305	299	644	9	10
Insurance (reinsurance) companies	261	539	550	406	161
Exchange offices				14	46
Pawnshops			1		14
Entities engaged in microfinance activity		7	6	28	9
Payment service providers		26	144	212	33
Non-bank e-money system operators	11				
Notaries	5	13	12	14	4
Bookmaker offices				3	1

810. No breaches of the TFS related obligations by DNFBPs and VASPs have been identified.

Higher risk countries

811. The lists of higher risk countries (the FATF “black” and “grey” lists and the sanction lists of the UN, OFAC and EU) are posted in the Personal Accounts of obliged entities on the FMA website. Besides that, STBS also use their own “stop lists” and the “red flag” lists developed by the ARDFM.

812. All FIs deny services to customers from countries included in the FATF “black” list, except for establishing business relationships with the Iranian citizens who have the permit to reside in Kazakhstan.

813. In general, FIs classify customers from FATF “grey list” countries or customers whose BOs reside or are registered in such countries as high geographic risk and apply appropriate risk mitigating measures, including enhanced CDD measures. At the same time, conducted interviews indicate that some FIs prefer not to establish or continue business relationships with such customers.

814. All DNFBPs are aware of the obligation to refuse to establish or maintain business relationships with customers from countries included in the FATF "black" list, except for business relationships with Iranian citizens who obtain a resident permit in Kazakhstan. The customer base of real estate agents and bookmaker offices is composed only of residents or individuals who are granted a resident permit in Kazakhstan. There have been no instances when business relationships were denied to customers from countries included in the FATF "black" list, as no such customers were encountered by the interviewed DNFBPs.

Case Study 4.3 (dealers in precious metals and stones)

The scoring analysis conducted by AK Company (jewelry company) in the first quarter of 2022 resulted in assignment of a higher country (geographic) risk degree to certain customers.

The higher risk degree was assigned due to the fact that those customers were located in the country that was identified by Transparency International as having a high level of corruption.

The contracts entered into by AK Company with those customers included, inter alia, the anti-corruption compliance clauses.

815. As for customers linked to other sanction lists (e.g. customers or counterparties who are residents of off-shore countries and territories), obliged entities assign higher risk ratings to such customers and apply enhanced CDD measures to them.

816. When establishing online business relationships, VASPs screen the countries of residence of each customer and its beneficial owner(s) against the sanction lists using the FMA and FATF lists integrated in their systems and databases. As no positive matches have been identified, no cases of refusal to establish business relationships with customers have been recorded.

5.2.5. Reporting obligations and tipping-off

817. All obliged entities have demonstrated a good awareness and general understanding of their obligations to report threshold and suspicious transactions to the FIU.

Table 4.4. Number of STRs Received by the FMA from Obliged Entries

Categories of Obliged Entities	2018	2019	2020	2021	2022
STBs	1,779	1,811,537	1,851,437	1,806,855	795,476
Central depository	50,361	49,869	47,225	21,440	9,713
Securities market participants	39,436	40,372	55,185	47,810	17,240
Entities engaged in certain types of banking operations	34,572	33,884	26,034	628	14065
Commodity exchanges	4,379	3,443	4,532	8,835	4,214
KazPost	2,063	2,814	3,822	4,195	2,174
Insurance (reinsurance) companies	1,633	2,504	3,739	1,502	537
Exchange offices	14 154	23 227	21 209	25 718	12 562
Pawnshops	2,159	4,696	7,679	7,765	4,960
Entities engaged in microfinance activity	847	1,742	1,459	3,274	1,466
Payment service providers	229	1,445	5,925	3,686	3,056
Insurance brokers	8	74	48		14
Credit partnerships			29	107	80
Third-party payment processors	673	166			
Non-bank e-money system operators	20	26			
Leasing companies	217	61	27	150	529
Notaries	22,755	10,980	7,955	13,102	15,565
Audit firms	985	777	729	2,070	2,557
Organisers of gambling industry	53	136	232		
Bookmaker offices			11	151	5,658
Casinos			10	119	202
Accounting firms and individual professional accountants		21	1	1	20

Individual and corporate dealers in precious metals, precious stones and jewelry	11	15	31	7	542
Individual and corporate real estate agents			1		4
AIFC member, incl.		531	332	21 735	7 715
FIs		531	332	21 716	7 692
VASPs				19	23

Table 4.5 Number of Threshold and Suspicious Transaction Reports Received by the FMA from Obliged Entities

Obliged Entities Sectors	2018	2019	2020	2021	2022
Financial Institutions					
Threshold transaction reports	998,251	1,089,126	1,158,194	1,427,716	723,878
Suspicious transaction reports	1,133,249	858,847	845,436	508,814	144,013
DNFBPs					
Threshold transaction reports	4,391	6,891	10,067	12,395	19,177
Suspicious transaction reports	21,572	9,734	6,674	14,034	10,343
AIFC Member Companies					
Threshold transaction reports		531	291	17,121	7,690
Suspicious transaction reports			41	4,614	25

818. Most reports received by the FMA are threshold transaction reports. However, certain categories of obliged entities, such as STBs (in 2018-2019), third-party payment processors, PSPs, non-bank e-money system operators, notaries (in 2018-2022), dealers in precious metals and precious stones (in 2019-2021), leasing companies (in 2018 and 2020-2021) and insurance (reinsurance) companies (in 2021), filed increased number of STRs. This trend is explained by the specificities of business activities of third-party payment processors and also by the large number of other transactions with cash and is consistent with the country's risks.

819. The relatively high number of STRs sent by STBs is due to the large number of transactions conducted and the broad customer base. At the beginning of the analyzed period, some STBs sent too many STRs without conducting sufficient pre-analysis for suspected ML/TF, but supervisory authorities applied the measures that resulted in a significant improvement in the quality of the STRs.

820. Lawyers and DNFBPs in AIFC file no reports with the FMA. This is partly due to the specificities of their activities, on the one hand, and scope of transactions they are required to monitor, on the other hand.

821. Certain obliged entities (insurance brokers in 2018-2020; credit partnerships in 2020-2022; organisers of gambling industry in 2018-2020; bookmaker offices in 2020; casinos in 2020 and 2022; accounting firms in 2019-2022; and real estate agents in 2020 and 2022) submitted no STRs. Limited number of reports filed by the AIFC members is explained by their specificity and small customer base.

822. Along with that, according to the information of ARDFM, the transactions carried out or monitored by insurance brokers do not, in most cases, meet the suspicion criteria set out in the legislation.

823. It is also noteworthy that failure to report or late reporting of suspicious transactions is one of the most frequently identified breaches of the AML/CFT legislation in relation to FIs (see Table 3.12 in Chapter 6). In many cases, violations are caused by technical failures of automated systems and human error. Also, untimely sending of STRs is partly due to the current wording of legal requirements on the timing of sending STRs. The FIs often recognises transactions as suspicious after the transaction has taken place, as there is a difficulty in deciding quickly whether to categorise a transaction as suspicious and then sending an STR before or within the legally prescribed time frame.

824. Certain FIs (STBs, PSPs, insurance companies, securities market participants) develop and use their own suspicious transaction indicators in addition to the indicators set out in the legislation. Other FIs (commodity exchanges, leasing companies, most EEMAs) apply a more rule-based approach to identification of suspicious transactions using the criteria established by FMA Order 13, and do not develop their own ML/TF suspicious indicators and typologies.

825. However, some of the interviewed obliged entities pointed out that the adopted indicators set out in Order 13 have been developed based on the practical operation of obliged entities and NRA results, and therefore currently do not require any modifications.

826. Besides that, certain obliged entities (STBs, pawnshops, PSPs, securities market participants, notaries) identify and report transactions that meet the ML and TF typologies. In 2019-2022, they filed a total of 283 such reports. Transactions that meet the TF typologies have been reported by STBs, pawnshops, PSPs and notaries, with 5 such reports filed in 2019 and 2021-2022.

827. On the other hand, it should be noted that some obliged entities (insurance companies, for example) do not identify suspicious transactions that meet the typologies published by the supervisors, as these typologies are not typical for their specific activities and reflect general vulnerabilities existing in the region, e.g. in the CIS member countries.

828. In view of general shortcomings in understanding of risks, most suspicious transaction reports filed by obliged entities are related to predicate offences and/or are associated with customers included in the sanction lists.

829. During the interviews all obliged entities demonstrated a good understanding of the confidentiality requirements and importance of avoiding disclosure of that fact that suspicious or threshold transaction reports or related information regarding their customers is being filed with the FIU.

830. Suspicious transaction reports are filed electronically using the FM-1 Form via the secure communication channels. Obliged entities use two systems for the transaction reporting purposes: manual report generating system (WEB-SFM system) and automated report generating system (ARM-SFM system which is fee-based and intended for processing a large number of transactions). The manual WEB-SFM system is used mainly by non-financial sector entities (notaries, organisers of gambling industry, real estate agents, etc.), while the automated ARM-SFM system is used by financial sector entities (STBs, exchanges, securities market participants, etc.). The WEB-SFM system is accessible to all obliged entities in their Personal Accounts on the FMA website and provides for automated completion of a report by selecting the listed options and also manual description of transaction details.

831. In order to prevent tipping-off, an employee of obliged entity shall sign a confidentiality agreement while being hired, that stipulates responsibilities. In addition, the MCS and organisers of gambling industry monitor privacy issues via IP addresses of employees' workplaces. In addition to the secure communication channel, the FMA differentiates access to information. The AFSA adopted regulations on personal data, as well as using security standards, and implemented requirements for third-party audits, secure storage of personal data, and knowledge checks of employees.

832. All obliged entities train their staff and develop detailed instructions on staff behaviors in the presence of the customer when a suspicion of AML/CFT is identified, so as to mitigate the risk of information leakage.

833. Automation of the STR generating and filing process, as well as institutional measures taken positively influence on the effectiveness in terms of accuracy of information and timeliness of data transmission.

5.2.6. Internal controls and legal/ regulatory requirements impeding implementation

834. All obliged entities perform internal control of business relationships and transactions of their customers. The internal control functions are distributed among officers of the relevant departments in all obliged entities, except for lawyers, accountants, notaries and real estate agents.

835. Most FIs and all AIFC members have automated internal control procedures in place, which include maintaining customer databases, assessing risks, screening customers against the lists and keeping transaction records. Nevertheless, the final decisions are made by the internal control officers.

836. According to the interviews most FIs regularly conduct internal audits of their internal control

systems, including AML/CFT systems. Large FIs regularly undergo external audits of their AML/CFT systems.

837. Members of financial groups apply group-wide internal control policies to the extent that they do not contradict the Kazakh legislation.

Case Study 5.4. (Shinhan Bank, Republic of Korea)

Assessment of exposure of the Bank to ML/TF risks is conducted with the use of a single methodology adopted by the parent company in the Republic of Korea. The Korean regulator conducts consolidated supervision of the group and requests, through the parent company, all necessary information, including AML/CFT information, from the group subsidiaries.

Case Study 5.5. (Brill Bank, China)

There is a three-stage transaction monitoring process in place: transactions are initiated and verified in Hong Kong office prior to their approval by the Bank before sending SWIFT messages. The centralized internal control of compliance with the AML/CFT procedures is also conducted in Hong Kong.

838. The exchange trading regulations require brokers to keep information about transaction parties confidential. However, this regulatory impediment is mitigated by the fact that exchanges themselves have access to information about all trading parties (i.e. customers of brokers and dealers). The insurance legislation does not prevent insurance companies from requesting the Financial Monitoring Agency to suspend payment of insurance compensations or terminating business relationships with customers in case of suspicious transactions.

839. No legal impediments for implementing internal controls by obliged entities have been identified. The work performed by the FMA and SRB largely contributes to implementation of internal controls.

840. All DNFBPs, including the AIFC members and VASPs, sufficiently implement the internal control procedures. All categories of DNFBPs and VASPs have developed and use the internal control rules in their day-to-day operations.

841. Most DNFBPs (except for real estate agents) and VASPs have automated internal control procedures in place, which include maintaining customer databases, assessing risks, screening customers against the lists and keeping transaction records. Nevertheless, the final decisions are made by the internal control officers.

842. In the course of on-site meetings with dealers in precious metals and stones, the assessors interviewed representatives of entities that are part of financial groups. These DNFBPs also apply group-wide internal control policies to the extent that they do not contradict the Kazakh legislation.

Overall conclusions on IO.4

Financial institutions

843. In the financial sector, most obliged entities have good enough understanding of AML/CFT obligations and risks existing in the country, sectors and their institutions. However, understanding of risks concerns primarily potential involvement in predicate offences, but not in ML/TF schemes (except for STBs, PSP and insurance companies).

844. FIs conduct CDD when establishing business relationships and perform ongoing monitoring of transactions carried out by customers and their beneficial owners, but the practice of applying standard, simplified and extended measures varies from sector to sector, as well as in individual obliged entities. The full range of CDD measures, depending on the risk level assigned to the client, is applied mainly in STBs, but to a lesser extent in other sectors. There are also shortcomings in identification of ultimate beneficial owners of corporate customers.

845. In general, FIs apply enhanced CDD measures to high-risk customers, but certain FIs prefer to refuse to establish or continue business relationships with high-risk clients instead of taking enhanced CDD measures.

846. Not all obliged entities identify and report suspicious transactions to the FMA, although this deficiency is observed in sectors exposed to a low risk where suspicious transactions are minimized.

847. The banking sector, which represents the largest and most significant sector of the financial system through which monetary transactions pass, is the most effective in applying preventive AML/CFT measures. The rest of the obliged entities tend to rely on the controls implemented by the STBs to conduct customer transactions.

DNFBPs and VASPs

848. In general, the DNFBPs have a good understanding of level ML and TF/PF threats and vulnerabilities in sectors. They also understand the level of national ML risks and, to a lesser extent, the level of national TF/PF risks. Sectoral ML/TF/PF risk assessments would allow to improve understanding of their own risk profiles.

849. VASPs have a good understanding of ML and TF/PF risks and also risks related to misuse of digital assets for ML/TF/PF purposes.

850. In general, DNFBPs and VASPs have demonstrated a significant level of understanding of the AML/CFT obligations in context of their sectoral specificities. The DNFBP and VASP sector entities implement internal controls and comply with the ICR requirements related to conducting customer due diligence and screening customers against the lists. Besides that, all DNFBPs and VASPs have demonstrated a good awareness of their TFS obligations and understanding of the need to apply targeted financial sanctions and to keep confidentiality. At the same time, there are shortcomings in identification of beneficial owners in context of transactions carried out by natural persons and also in identification of domestic PEPs, since these requirements have been implemented in the AML/CFT Law relatively recently. All demonstrated understanding and knowledge of the need to identify and report suspicious transactions/activities to FMA.

851. **Kazakhstan is rated as having a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

6.1. Key findings and recommended actions

Key findings

Financial institutions

1. FIs activity covered by the FATF standards requires to be licensed or registered in Kazakhstan for the purpose of AML/CFT compliance monitoring and supervision by supervisory authorities, and supervisory authorities conduct regular inspections to identify unlicensed or unregistered activities.

2. Supervisors effectively identify cases of criminals owning significant shares in FIs as well as holding managerial positions, but do not identify persons affiliated with criminals. Besides, the NB and APDC verify the resident BOs of FIs against state databases, where information is not checked for accuracy.

3. Except for APDC, supervisory authorities know and understand well the existing risks in the country, including through conducting sectoral risk assessments, but this understanding generally relate to the threats of predicate offences and the involvement of different obliged entities in them rather than the specific ML/TF risks of obliged entities.

4. ARDFM and NB have most effectively applied various tools of risk-based approach in supervising the compliance of FIs with AML/CFT requirements, including on-site inspections and unplanned inspections and remote supervision. The APDC applied risk-based supervision to a lesser extent. However, there is no practice of consolidated supervision of an international financial group in the ARDFM. In addition, the period between inspections (1 to 3 years) appears to be quite short, given the average length of the supervisory cycle and the risk profile of Kazakhstan.

5. Supervisory authorities generally apply a wide range of corrective measures when complying with AML/CFT requirements. Nevertheless, the statistics provided as well as the existing system of imposing administrative fines do not allow to conclude that these measures are proportionate to the violations committed and sufficiently effective to prevent subsequent violations of AML/CFT legislation by other obliged entities.

6. Supervisory authorities (except for APDC) generally conduct regular AML/CFT training of their personnel.

7. Supervisory authorities also proactively interact with FIs to enhance their understanding of the requirements and obligations prescribed by the AML/CFT laws.

DNFBPs and VASPs

8. With the exception of lawyers, notaries, legal advisors and real estate agents, all DNFBPs shall be registered as legal entities. Lawyers, notaries, legal advisors, audit firms, casinos and organisers of gambling industry shall be licensed. Jewelers, legal advisors, real estate agents shall notify FMA about commencement of activities as obliged entity.

9. The DNFBP sector and VASPs outside AIFC has certain mechanisms in place to prevent criminals from entering the market, both at the moment of registration or licensing for a few sectors and at the moment of notification of FMA as an obliged entity. At the moment of registration, the founders and managers of DNFBPs – legal entities are checked against the lists of organisations and persons associated with FT, extremism and PF.

10. The AFSA registers and licenses AIFC members that are DNFBPs and VASPs, and identifies BOs and affiliates, and checks for criminal history, sanctions, etc.

11. FMA, MCS, IPAC, MoJ generally demonstrated good awareness of threats and vulnerabilities at the sectoral level. The lack of sectoral assessments limited to some extent the understanding of risks. FMA and AFSA have a good awareness of threats and vulnerabilities in the supervised sectors and have a good understanding of risks.

12. FMA, MCS, IPAC, MoJ apply elements of risk-based supervision. The criteria for selecting do not take into account the type and number of entities in the sector. The Council of the Bar Association is responsible for organizing AML/CFT for lawyers, and should analyze and monitor their activities in order to identify risks and comply with AML/CFT legislation starting from July 1, 2022. Nevertheless, this work had not commenced yet as of on-site mission. The AFSA demonstrated a good model of RBA in supervision.

13. The corrective measures applied by FMA, MCS, IPAC, MoJ are more of a preventive nature. Corrective measures are not diverse, and sanctions are not proportionate and dissuasive.

14. AFSA applies various corrective measures, including to AIFC obliged entities' officials. At the time of the on-site mission, no inspections have been completed, up to and including the determination and imposition of sanctions and corrective measures on AIFC members.

15. FMA plays a leading role in enhancing understanding of the AML/CFT obligations. Supervisory authorities rely more on FMA and sectoral SRBs with respect to training and monitoring of the AML/CFT activities of obliged entities.

Recommended actions

Financial institutions

1. Supervisory authorities should expand the scope of the checks of the business reputation of major shareholders and executive officials for their affiliation with criminals.

2. The NB and APDC should increase the number of data sources on resident BOs and do not solely rely on government databases.

3. Supervisory authorities should understand not only risks of obliged entities' involvement in predicate offence, but also the risks of their involvement in laundering of proceeds from predicate offences and take measures to mitigate these risks.

4. It is recommended that ARDFM and NB reconsider the appropriateness of mandatory scheduled inspections at intervals of 1 to 3 years, taking into account the risk profile of the supervised obliged entities.

5. APDC should on a regular basis conduct random on-site inspections of commodity exchanges to make sure that they do not violate the AML/CFT laws.

6. Supervisory authorities are recommended to apply general indicators of impact of supervisory response measures on obliged entities' compliance with the AML/CFT requirements to assess efficiency of the taken measures.

7. APDC is recommended to regularly conduct AML/CFT training of its personnel and include training activities in the annual work plan.

DNFBPs and VASPs

8. To better understand the ML/TF/PF risks and risk-based supervision approaches, supervisory authorities should consider conduct of sectoral assessments.

9. Supervisory authorities should take additional measures to extend the requirements to all categories of DNFBPs to prevent criminals and their affiliated persons from beneficial owning and holding executive positions.

10. Supervisory authorities should consider inclusion in risk management systems some AML/CFT/CPF statistics taking into account the findings of the NRA and the characteristic features of the activities in the sectors in order to complement the criteria for selecting entities for inspection with quantitative and qualitative indicators.

11. Supervisory authorities should involve SRBs more actively in supervision/monitoring activities.

12. It is recommended to correct measures to apply administrative sanctions, *inter alia*, to the officials of DNFBPs that violated the requirements of the AML/CFT laws as well as expanding the range of corrective measures.

13. AFSA should pay attention to the measures to enhance DNFBPs and VASPs' understanding of their AML/CFT obligations.

852. This Chapter reviews and assesses the achievement of Immediate Outcome 3. To assess efficiency, this section used Recommendations 14, 15, 26-28, 34 and 35, as well as the elements of R.1 and 40.

6.2. Immediate outcome 3 (Supervision)

6.2.1. Licensing, registration and other types of control that prevent criminals and their accomplices from entering the market

853. The assessment and conclusion on IO3 is based on interviews with the supervisory authorities in Kazakhstan, statistical data and case studies provided by the country. Institutional structure of supervisory authorities is presented in the Table F (see para 204).

854. For the purpose of the effectiveness assessment, the important obliged entities include STB, securities market participants, EEMA, postal operator, dealers in precious metals, precious stones and jewelry, real estate agents, organisers of gambling industry. Sectors of insurance (reinsurance) companies, payment service providers, leasing companies, exchange offices run by authorized institutions, notaries, accounting firms and professional accountants, VASPs are identified as moderately important. And the entities engaged in certain types of banking operations, commodity exchanges, lawyers, legal advisors, other legal professionals, audit firms and AIFC members (except for VASPs) were weighted as being of low importance (see para 168-195 of the Report).

Financial institutions

855. Controls on the entry of FIs into the market are quite effective in most sectors. The licensing and registration process is reasonably robust, and the supervisory authorities systematically screen major shareholders and managers when licensing or registering or inspecting, in order to prevent criminals from entering the market. There are no refusals of licensing the obliged entities or issuing a consent for appointment of executive officers, except for certain cases. Despite, the cited examples of the identification of, as well as late notification of changes of major shareholders and managers who do not meet the business reputation requirements, allow to conclude that the prevention of criminals holding major shares in FIs and performing management functions is quite effective. Supervisory authorities also check regularly to detect, and FIs report suspected unlicensed or unregistered activities.

856. However, the supervisors do not check the founders and managers of FIs for affiliation with criminals, and the NB and APDC check business reputation of resident BOs of FIs through a database where information is not checked for accuracy, which is a vulnerability in the controls.

857. There are two phases of entry into the FIs market. To become legal entities or individual entrepreneurs, all FIs should pass state registration (see Chapter 7). During registration, the business reputation of founders and managers is checked, including for the lack of outstanding or unexpunged conviction for offences related to bankruptcy, as well they are checked against the list of persons linked to terrorist and extremist activities.

858. The FIs are then licensed or pass through record registration to perform their activities.

859. AFSA grants FIs in AIFC appropriate licenses for the declared type of activity.

860. In the course of licensing or record registration, appropriate government authorities check the business reputation of founders and their BOs, as well as the managers of new FIs. Subsequently they check business reputation when major shareholders and/or managers change, as well as during inspections.

861. "Founders" mean major shareholders whose shares account for more than 10%. From 2022, the business reputation of the founders of PSPs are checked regardless of their shares. However, at the time of on-site mission supervisory authorities (except for AFSA) did not check the affiliation of the founders and managers of obliged entities with criminals.

862. In this context, spotless business reputation means the lack of outstanding, unexpunged convictions or court judgments related to illegal activities, honesty, professional competence, non-inclusion in the lists of persons linked to terrorism or extremism, no signs of residency in offshore zones and in the countries included in the FATF lists. Lack of residents' criminal record is checked against the databases of the Committee for State Statistics under the General Prosecutor's Office of the RK that may be accessed by all government authorities. ARDFM, NB and AFSA also check the sources of investments into newly established obliged entities.

863. Meanwhile, it is worth noting that NB commenced to check major shareholders of PSPs and AIs against the list of entities and persons involved in the FT and extremism and/or PF, as well as for being registered in offshores, from September 2022.

864. NB and APDC check business reputation of resident founders/major shareholders and BOs and managers, through government databases. ARDFM additionally utilizes open sources including commercial databases.

865. In order to check business reputation ARDFM requests the copies of apostilled and translated criminal record certificates in respect of non-residents who are founders/major shareholders, BOs or managers, and shares information with foreign regulatory authorities and uses open source information. NB sends international requests via FMA. For instance, during the period under review two non-residents were not appointed to executive positions based on international requests.

866. During the period under review, ARDFM refused to issue license to EEMAs 17 times within 2021-2022 years due to its managers/major shareholders' criminal records. And the overall number of applications received was 1,422.

867. ARDFM have not refused to issue license to other supervised obliged entities due to the lack of spotless business reputation except for two instances when non-resident persons were not appointed to the executive positions in existing STBs (in 2018). Nevertheless, ARDFM imposed supervisory measures (penalty) due to the late agreement upon the change of the major shareholder of a financial group that included STB, insurance company and securities market participant. The absence during the period under analysis of license denials due to non-compliance with business reputation requirements by major participants and senior executives of STBs, insurance companies, EEMAs and securities market participants is due to the absence or small number of applications.

868. NB have not refused to issue license to AIs, to register PSP or to appoint a manager due to the absence of a business reputation, despite the relatively high number of applications (223 and 352 respectively). There were also no refusals of licenses or appointments to managerial positions due to the lack of business reputation for commodity exchanges during the analyzed period, which is explained by the small number of applications.

869. In the analyzed period the AFSA issued one decision refusing to appoint a manager, including due to the person's involvement in corruption offences, and two warnings for failing to approve a change in the managers of the obliged entities. AFSA also identified a founder who was a relative of a person convicted

of corruption offences and issued a recommendation to the obliged entity to replace the founder accordingly.

870. ARDFM and NB identify and submit to LEA information on unlicensed activities based on information from supervised FIs, media and social media, as well as from individuals' complaints. The LEA react in a timely manner (from several days up to two weeks) and prevent those activities. In between 2018 and 2020, they detected 2 cases of unlicensed activities in the securities market. Since 2020, ARDFM has sent information to LEA on more than 350 different entities and persons, including information received from STBs. NB also regularly identifies through its branch offices the deficiencies in AIs activities. There were no examples of detection and suppression of unlicensed activities of the PSPs due to no possibility to provide payment services without direct interaction with the STBs, and the STBs should not establish business relationships with entities not having status of a PSP.

871. AFSA checks the business reputation of the founders, managers and beneficiary owners of FIs when it grants appropriate status to them. Data are checked through open sources, international and domestic databases and the sanction lists of Kazakhstan and UNSC. During registration of branches and subsidiaries, also requests information from foreign supervisory authorities to check the business reputation of parent companies.

Case study 3.1

In the course of registration of a company that is a member of AFSA in November 2018, it was identified that according to the data submitted by the applicant, the company's founder is a legal entity incorporated in England.

Following the check of the Incorporation Certificate, official of AFSA verified the founder's details against the registration details specified in Companies House (UK) public register, which is an open source.

In addition, the information on the beneficiary owner submitted by the applicant was verified against Companies House (UK) public register. Two natural persons were specified as ultimate beneficiary owners.

DNFBPs and VASPs

872. All DNFBPs (except for lawyers, notaries, legal advisors and real estate agents) should be registered as legal entities or individual entrepreneurs (see Chapter 7). In addition to registration, casinos, gaming machine halls, bookmaker offices, totalizators and audit firms must obtain a license. Lawyers and notaries also obtain licenses. Besides, in order to start and subsequently carry out activities or actions (operations) of a notary, organisers of gambling industry the individuals and legal entities need to notify the MoJ and the MCS respectively. In order to start activities as obliged entity legal advisors, jewelers, real estate agents need to notify FMA on the commencement of activity as an obliged entity. In order to start operating an accounting firm, it is required to undergo state registration and obtain a certificate of accreditation (issued for a period of 5 years). An individual professional accountant must hold a certificate of professional accountancy (issued for 3 years) and must be a member of a professional accounting organisation.

873. During state registration, legal entities may not be registered/re-registered if their founders/members and/or managers are included in the list of organizations and natural persons linked to financing of proliferation of weapons of mass destruction and/or the list of organizations and natural persons linked to financing of terrorism and extremism in accordance with the laws of the Republic of Kazakhstan.

874. Licensing authority checks the lack of criminal records when license is sought to conduct activities of lawyers or notaries, casinos, slot parlors and bookmaker offices. Persons that have conviction that is outstanding or unexpunged in the manner prescribed by law may not act as legal advisors.

875. However, natural persons that do not have outstanding or unexpunged convictions for economic, as well as intentional medium gravity, grievous or extremely grievous offences may not be appointed to the

executive positions of DNFBPs.

876. FMA receives notifications of the commencement of activities as an obliged entity from four categories of the obliged entities. It maintains a register of obliged entities that have submitted notifications and a register of obliged entities that have submitted threshold and suspicious transaction reports (STRs/SARs). Based on these registers, the FMA conducts its own due diligence on the involvement of managers and beneficial owners in ML/TF according to the list of entities and individuals involved in the financing of proliferation of weapons of mass destruction (the PF list), the list of entities and individuals involved in the financing of terrorism and extremism (the TF list) and the list of unified register of high-risk entities (URHRE list).

877. As the result of FMA inspections, in 2020 141 matches with the persons subjected to court rulings and decrees (prohibitions), 1 match with a person related to FT and 940 matches with the persons that have outstanding or unexpunged convictions were identified. The said persons and entities were refused to be registered or their registration was canceled.

878. Legal advisors, jewelers and real estate agents notify FMA about the commencement and completion of their activities as an obliged entity through E-Licensing web-portal. If obliged entities conduct activities without such notification, they should be brought to administrative liability. In 2021 and 2022 FMA detected 9 violations of notification procedure in 2021 and 8 violations in 2022 as part of preventive control. The violators were notified to eliminate the violations with the term of execution from 2 to 3 months. There are facts of non-execution of the notifications, in connection with which the administrative penalties under Part 3 of Article 462 of the Administrative Code in the form of a fine of 200 MCI (~ $ 1,300) were imposed on medium-sized businesses. In addition, a fine of 500 MCI (~ $3,300) has been imposed on large businesses.

879. Before the commencement of audit activities, audit firms should be licensed by IPAC. For this purpose, it should comply with licensing requirements and the auditors should comply with certain qualification requirements. Licensing requirements do not contain provisions that prescribe criminal record checks. There are cases of refusal to issue a license if there is a court decision (sentence) to suspend or prohibit activities.

880. However, before issuing licenses IPAC practically checks the details of license applicants against the database of Legal Statistics Committee of the General Prosecutor's Office, which is integrated with E-Licensing government information system and allows to verify the ownership of share funds of the shareholders of the audit firms, and Judicial Office database that contains data on perpetrators, suspects, accused, detained or arrested individuals.

881. The organisers of gambling industry may not be (directly and/or indirectly own, use, dispose of and/or manage the shares /(interests in the charter capital of legal entities) legal entities whose founders, shareholders or BOs have outstanding or unexpunged conviction for economic or intentional medium gravity, grievous or extremely grievous offences.

882. Persons that have high education, gambling work experience of no less than two years and impeccable business reputation may only occupy the position of the heads of the organisers of gambling industry.

883. When licensing applications are considered, the details of founders, managers and BOs of legal entities are checked for criminal records through Judicial Office database for inclusion in the lists of persons that FMA maintains (updates and provides access to supervisory authorities).

884. To obtain the details of founders, shareholders, managers and BOs, MCS examines the constituent documents submitted by applicants, verifies them against State Databases "Natural Persons" and "Legal Persons" maintained of MoJ, databases of Committee for Legal Statistics and Special Recording of the General Prosecutor's Office and submits requests to gambling associations. If any suspicions in the authenticity of data arise, respective SRB (Association) assists in obtaining reliable data.

885. In addition, MCS refused to register or license organiser of gambling industry as well as to suspend

of license. There were no instances of refusing due to convictions of founders, participants, managers and BOs.

Table 3.1. MCS's suspension of licenses and denials of licensing

	2018	2019	2020	2021	2022
Suspensions	3	1	2	4	1
Denials	8	7	11	9	7

886. In 2018, 2019, 2021, 2022, licenses were suspended by the MCS on the basis of applications for voluntary suspension of the license, in 2020 – by court decision due to a violation under Article 464 (violation of licensing regulations) of the CAO.

887. If the BO of an organiser of gambling industry has an unexpunged criminal record, this organiser is monitored for one year.

888. Given that online casinos are prohibited in the country, Kazakhstan has taken effective measures to identify and ban such content (see case study 5.5).

889. MoJ as a licensing authority checks the details of licensee applicants (lawyers and notaries) through government databases, including State Databases "Natural Persons" and "Legal Persons" and if there is a court conviction, repeated violation of the law and ethics, take action to suspend, terminate, or revoke the license.

Table 3.2. Information on the suspension, termination, and revoking of notaries licenses

	2018	2019	2020	2021	1 пол. 2022
Suspension	32	52	45	17	11
Termination	5	11	11	12	7
Revoking	-	1	2	2	6

Table 3.3. Information on the suspension, termination, and revoking of advocates licenses

	2018	2019	2020	2021	1 пол. 2022
Suspension	1	3	3	2	-
Termination and Revoking	6	10	14	16	6

890. Members of AIFC, including VASPs, should be registered with Ministry of Justice and obtain appropriate licenses for the declared type of activities from AIFC. When status of the members of AIFC, including DNFBPs and VASPs, is granted, AFSA checks the business reputation of their founders, managers and beneficiary owners. Details of beneficiary owners and managers are identified and examined in several stages, including:

- Mandatory disclosure of ultimate beneficiary owners and persons that exercise indirect control;
- Disclosure of the beneficiary ownership structure and beneficiary owners whose share in authorized capital exceeds 20%;
- Collection of data on financial solvency and sources of funds, including those to form authorized capital;
- Checks for managers' professional compliance and fitness through national and international databases and interviews. Interviews with applicants are adapted to each category of obliged entities registered with AFSA.

891. AFSA exercises post-licensing control of the obliged entities that are the members of AIFC, including VASPs, through regular collection of reports and interaction with competent and other law enforcement authorities.

Case study 3.2

In the course of regular examination, AFSA, through checks of open sources, has identified that Mr. A.,

who is a beneficiary owner of the DNFBP already registered with AIFC is suspected in involvement in financing of illegal activities.

On 11.07.2022, the AFSA informed the FMA. In turn, FMA conducted an additional check and on 22.07.2022 informed the AFSA that a criminal case was initiated against citizen A.

In addition, the AFSA conducted a check on the affiliation with other member of the AIFC with regard to the DNFBP and citizen A. Citizen A. was found to be affiliated with another AIFC member carrying a non-financial activity. This company was registered a year later than the DNFBP. At the same time, there was no negative information about citizen A. at the time of registration.

The AIFC members affiliated through citizen A. were placed under enhanced monitoring. The AFSA analysed the operational and financial activities of both legal entities and found no activity since registration.

Both AIFC participants have been placed on the list of forthcoming on-site inspections (corporate matters).

Upon completion of the ongoing investigative activities in relation to citizen A. the AFSA will decide whether it is necessary to change the ownership of the two AIFC participants or to terminate their activities on the AIFC premises.

892. In addition, in the course of interagency interaction AFSA and MDD make efforts to identify the VASPs that conduct unlicensed activities in the country. In 2021-2022, AFSA identified 37 illegal VASPs; the government authorities of the RK were notified thereof and measures were taken to terminate their activities. Joint discussions are underway to block websites of crypto exchanges not licensed by the AFSA. Thus, by letter No. AFSA-G-EC-2022-0010 of 26.09.2022, AFSA informed MDD of the lists of licensed (legal) crypto-exchanges and VASPs, and unlicensed crypto-exchanges whose websites are subject to blocking.

893. VASPs that are not AFSA members should notify Ministry of Digital Development, Innovations and Aerospace Industry on the commencement of their activities, at the time of the on-site mission there were no these notices.

6.2.2. Supervisory authorities' understanding and identification of ML/TF risks

Financial institutions

894. In general, supervisory authorities, including AFSA, are well aware of the ML threats and vulnerabilities of the supervised sectors and have a good understanding of the national risks. However, ARDFM, NB and AFSA have a more in-depth view on the risks of the supervised sectors due to sectoral risk assessments conducted separately from NRA and the risk profile assessments of the obliged entities. The understanding of TF risks is less in-depth, as the SRA have not analysed TF risk for different sectors separately from ML risk, and supervisors focus on the NRA for TF (see IO.1). Supervisors consider the risk of the involvement of FIs, with the exception of Kazpost, to be low.

895. Development of ML typologies confirms that supervisory authorities understand ML threats and vulnerabilities. ARDFM has consolidated the most typical signs of the transactions related to ML offences and has developed indicators to identify them. The typologies analyses of the identified ML typologies, including those developed on the basis of information received from other countries' supervisory authorities, are available on the NB web portal.

896. In 2022, ARDFM и NB, in cooperation with FMA, compiled a list of transactions that should be treated as ML/FT typologies, schemes and types (the Order 13).

897. However, the majority of typologies and signs of suspiciousness relates to involvement to predicate offences. Also, during the period under review ARDFM и NB did not identify obliged entities' involvement in ML/TF schemes, which may demonstrate their insufficient understanding of ML/TF risks.

898. Supervisory authorities develop Risk Mitigation Plans to be approved together with FMA. Mitigation measures focus on application of preventive measures to mitigate the risks of predicate offences

899. NB is well aware of and understands the ML risks specified in the NRA report as both first and second NRAs were, *inter alia*, based on the assessment of threats and vulnerabilities identified by the NB during its supervision of respective FIs. The NB also has a good understanding of the risks of supervised FIs and takes into account the results of the NRA in the assessment of individual risks of PSPs and AIs, and NB revises those risks on an ongoing basis based on the results of inspections conducted, breaches identified and supervisory measures taken. Following the 2021 NRA and the sectoral risk assessment that NB conducted in 2022, the methodologies of the risk level assessment of PSPs were updated to draw up a list of high-risk payment institutions to conduct inspections; the list of the signs of suspicious transactions was expanded.

900. Following the 2018 and 2021 NRAs, legislative measures were taken to exchange offices to mitigate the risks, including total recording of identification data regardless of transaction amounts.

901. ARDFM is well aware of the risks specified in the NRA report and was directly involved in collection and review of documents during the process of its preparation. ARDFM demonstrates a solid understanding of the vulnerabilities of the reporting sectors due to the fact that in 2021 it conducted sectoral risk assessments. In 2020-2022, ARDFM, in cooperation with FMA and NB took a number of measures to mitigate the risks identified in the NRA: enhancement of financial monitoring measures to prevent illegal cross-border financial transactions; recommendations to identify the signs of the offences committed through foreign trade contracts; tightening the due diligence of STBs in respect of large conversion transactions in cashless form; recommendations for banks to enhance control of cross-border money transactions; generation of reports of the turnover of the money lent by banks with a breakdown into branches, etc.

902. However, taking into account the general deficiency of the NRA for ML (see Key finding 2 in Chapter 2), the measures taken by ARDFM и NB to mitigate the risks generally relate to the threats of predicate offences (fraudulent activities, Ponzi schemes and siphoning of capital). For example, as a result of an ARDFM inspection, a case was identified where funds sent for risk reinsurance by a non-resident entity of Kazakhstan were not fully confirmed due to the participation of a “chain” of foreign intermediaries in the transaction. In order to regulate the external reinsurance system in 2018, the RK has adopted legislative initiatives: i) to prohibit the participation of several non-resident insurance brokers in reinsurance of one risk; ii) to introduce a blacklist of reinsurance companies and non-resident insurance brokers; iii) to tighten requirements for formation of the reinsurer share in insurance reserves.

903. During the assessment the country specially emphasized the involvement of EEMAs in criminal activities, which is explained by insufficiently automated processes for this category of obliged entities.

904. As a result of measures taken by the authorities, the number of registered internet frauds decreased from 11759 to 9608 in the first six months of this year compared to the same period last year.

905. According to the information provided by the EEMAs, there were 3726 cases of fictitious micro-loans from 2020 to 1 July 2022.

906. Thus, in order to counteract the activities of internet fraudsters, the following activities were carried out by the ARDFM.

- The licensing process has been completed. As of July 1, 2022, 217 credit partnerships, 581 pawnshops and 246 microfinance organisations were licensed. The number of EEMAs providing online microcredit in 2022 was 42, an increase of 41% compared to 2020.
- In February 2021, supervisory response measures were applied to 21 EEMAs issuing online loans by ordering them to stop providing microcredits electronically without biometric identification or identification by means of electronic digital signature.

- In March 2021, the Agency obliged all EEMAs providing online loans to ensure the actual verification and confirmation of client authenticity, verification of client data against the data specified in the application, compliance of client's actual biometric data with the data specified in the identity documents, as well as recording the will of the client to receive a microcredit when granting new microcredits.
- pursuant to the resolution of the Board of the Agency dated 30.04.2021. No. 63 introduced a new procedure for identifying borrowers when granting microcredits online.
- Resolution No. 108 of the Board of the Agency of 13 December 2021 introduced additional methods of authentication through reconciliation with the data of mobile operators.

907. As a result of the measures taken by ARDFM, 115 cases were recorded in H1 2022, compared to 841 cases in the same period of 2021, which in turn shows an 86.3% reduction in the number of frauds.

908. APDC has demonstrated insufficient understanding of the national risks in general and of the reporting sector specifically. Risk mitigation measures do not relate to the specific ML/TF vulnerabilities of commodities exchanges (integration of web-sites and electronic trading systems of commodities exchanges with the information system of One-Stop Shop web-portal is under way to enhance the transparency of the exchange transactions and provide access to trades for the maximum amount of potential market players). Also, there are no typologies of commodity exchanges' involvement in ML/TF.

909. In 2021, FMA conducted the risk assessment of the leasing sector. Following the assessment, the sector received medium risk level due to the fact that the knowledge and experience may be used in ML schemes, although leasing companies' involvement in ML-related offences has not been identified. FMA has developed and generally takes preventive measures.

910. AFSA has demonstrated a solid understanding of the vulnerabilities of the obliged entities during the sectoral risk assessment and the vulnerabilities of involvement of the FIs that are AFSA members in ML/TF schemes.

911. In 2021, AFSA conducted the ML/TF risk assessments of the financial sector. Following the assessment, the FIs in AIFC received medium risk level which seems adequate given the rather risky range of services and the client base of FIs in AIFC (banking, securities market services, non-resident clients), but rather low activity due to the short existence of AIFC since creation.

DNFBPs and VASPs

912. In general, the authorities responsible for supervision of DNFBPs have demonstrated a good knowledge of the threat and vulnerabilities of the reporting sectors; they have a basic understanding of national risks despite the absence of sectoral risk assessments. Based on the interviews, the assessment team concluded that the supervisors have sufficient knowledge of the risks in the supervised sectors.

913. In the course of the NRA for ML and NRA for TF/PF in 2021, government authorities observed supervised sectors, taking into account the findings of both NRA for ML and TF and using various criteria: types of activities, size of entities, transactions conducted, ML and TF cases investigated, compliance with AML/CFT requirements, implementation of supervisory measures. All categories of DNFBPs participated in the NRA 2021. Involvement of obliged entities was maximized via respective sectoral associations, while organisers of gambling industry, notaries, and audit firms were covered fully.

914. In 2021, FMA acted both as the coordinator of NRA for ML and NRA for TF/PF and as a regulatory authority of five categories of obliged entities, including leasing companies. FMA conducted extensive outreach and training activities. The evaluators assume that this work enabled FMA to the greatest extent demonstrate understanding of the general threats, vulnerabilities and risks of the reporting sectors.

915. Based on the findings of the NRA for ML and NRA for TF/PF, supervisory authorities in cooperation with FMA have developed Risk Mitigation Plans. The plans are generally related to the implementation of preventive measures aimed at mitigating the risks of predicate and ML/TF offences.

916. Casinos and other organizers of gambling industry are classified as high risk for ML and medium risk for TF. This is due to, *inter alia*, the existence of ML through bookmaker offices, numerous illegal casinos and totalizators. The MCS has demonstrated well awareness of and understanding these threats and vulnerabilities in the supervised sector.

917. In order to mitigate the high risks identified, the MCS has taken a number of measures, including lowering the cash winnings threshold to KZT 1 million (~$2,000) and reducing cash acceptance to 10% of the reported bet, which is broadly in line with the identified national risk of significant cash turnover in the country.

918. In addition, MCS carried out the inspections of organisers of gambling industry for compliance with Kazakhstan's gambling and AML/CFT legislation as part of the risk mitigation actions. Thus, it conducted 2 inspections in 2019 and 1 inspection in 2022. No AML/CFT violations were identified as a result of the inspections.

919. Being a supervisor for the accountants, realtors, jewelers and legal advisors, the FMA demonstrated a good understanding of threats, vulnerabilities and knowledge of national and sectoral risks. The legal advisors sector was assigned a low ML risk level. The medium risk level in NRA 2021 for the accountants, realtors, jewelers sector is due to the knowledge and expertise of accountants being utilized in tax crime schemes, complex financial transactions; the possibility of settling real estate in cash and using real estate as a ML target; the existence of illegal jewelry due to the detection of counterfeit jewelry workshops with fake branding.

920. FMA has developed measures to mitigate risks of the reporting sectors, which are implemented in four areas: regulation (procedure that prescribes a notification of the commencement of activities and registration, government control and inspections); methodology and rulemaking (revision of the AML/CFT Law and elaboration of regulations), interaction (maximum possible coverage of the obliged entities in cooperation with SRBs, with which 19 agreements have been concluded) and coordination, including through the web Personal Account developed by FMA, whose importance and usefulness were highly appreciated by all categories of obliged entities including by those that are accountable to other supervisory authorities.

921. IPAC demonstrated a moderate level of understanding of the ML/TF threats and vulnerabilities posed by audit firms, as well as moderate awareness of the risks in supervised sector. The audit firms were assigned a low level of ML risk as a result of the NRA 2021. However, it should be noted that due to the lack of audits, the absence of ICR in some entities, the lack of reporting of threshold and suspicious transactions, the sector was assigned a high risk level as a result of the NRA 2018.

922. Following the preventive work and control activities, the IPAC developed a departmental action plan to mitigate risks and to improve AML/CFT efficiency for 2022-2023 (No.14 dated 21.01.2022), aimed mainly at conducting training, AML/CFT control activities, which in view of the identified risk level seems to be sufficient.

923. Based on the ML and FT/PF NRA, these categories of DNFBPs (notaries and lawyers) to be licensed by Ministry of Justice received a low risk level, like in 2018. However, taking into account the measures to avoid the sectors' involvement in ML/TF processes taken by Ministry of Justice, it is assumed that understanding of the risks is limited to taking preventive measures aimed at explaining the requirements of AML/CFT legislation and training. It is worth mentioning the action plan developed by the FMA and the MoJ, which is aimed at ensuring compliance with AML/CFT legislation by the obliged entities. This plan envisages cooperation between the MoJ and the FMA, keeping, updating and transferring to FMA the records of notaries, lawyers and legal advisors; notification on AML/CFT violations of notaries; identification and analysis of AML/CFT risks in the activities of notaries, lawyers and legal consultants; development of measures aimed at minimizing the identified risks, participation of the MoJ in the development of recommendations and instructions for risk assessment in the sectors under its control. At the time of the on-site mission, the websites of the MoJ, local justice authorities, National Bar Association

and Notaries Chamber contained up-to-date lists of notaries, lawyers and legal advisors.

924. AFSA demonstrated good awareness and understanding of the threats, vulnerabilities and risks in the supervised sectors as well as in the digital assets sector. When assessing AFSA's understanding of the level of ML/TF risks, the Assessment team took into account the low level of involvement of VASPs in AIFC and DNFBPs in AIFC in the economy of Kazakhstan and their low level of activity during the analyzed period. AFSA demonstrated a good understanding and knowledge of the threats, vulnerabilities and risks in general in relation to DNFBPs and VASPs. This was supported by sectoral risk assessments and AML/CFT risk analysis related to the use of digital assets in AIFC. All supervised DNFBPs and VASPs participated in the assessment process. Director General of AFSA approved the report on digital assets risk assessment on 24.12.2021.

925. Following the assessment, DNFBPs and VASPs that are the members of AIFC received a medium risk level. Risk of using digital assets (cryptocurrency) within AIFC is also medium.

926. The AIFC has a policy document, the risk mitigation action plan for 2021-2022. It includes a set of 32 measures to improve regulation of digital assets, inter-agency cooperation, supervision and training. Besides, Memorandum on AML/CFT mutual understanding and cooperation and information sharing concluded between AFSA and FMA on October 18, 2021 also facilitated mitigation of the identified national ML/TF risks. At the time of the on-site mission, under the Memorandum AFSA sent 5 notices of unscrupulous practices and the persons involved; 6 interagency workshops were held; 10 joint events to raise awareness and implement rulemaking initiatives; 44 inspections were initiated based on FMA's notices.

927. AFSA continuously works on the analysis of ML/TF vulnerabilities and threats through the implemented risk-based regulatory and supervisory model for AIFC members, an ongoing information exchange has been established with the FMA

928. MDD has not participated in the work on the ML NRA and FT/PF Reports due to the fact that government control of VASPs outside AFSA was introduced in 2022. In 2020, legislative measures were taken to these services to mitigate the risks, including those that prescribe possibility of selling only secured crypto-assets in the Republic of Kazakhstan.

6.2.3. Risk-based supervision of compliance with AML/CFT requirements

929. Supervisory authorities applied various tools to supervise the compliance of FIs with AML/CFT requirements, including on-site inspections, unscheduled inspections and desk-based supervision, nevertheless they applied the risk-based supervision with varying degrees of effectiveness, depending on the sector.

Financial institutions

930. Legislatively, a risk-based approach to supervision in general (including prudential supervision and supervision of ML/TF compliance), governing risk-based inspections, was introduced in 2019 for the ARDFM and NB. Based on that, ARDFM and NB developed and approved in 2019 and 2020 the methodology to assign ML/TF risk level to each obliged entity based on qualitative and quantitative indices and to compile an examination sheet. Before, the NB utilized the Methodological recommendations on inspections for availability and compliance of internal documents, procedures and automated systems of financial institutions with AML/CFT legislation from 2014, which were based on a risk matrix that took into account quantitative indicators of obliged entities, qualitative risk assessment based on the AML/CFT questionnaire and results of conducted inspections.

931. For FIs that are supervised by ARDFM, quantitative indicators determine risk level; they include the size of FI (volume of assets and transactions), structure of customer base and products; they are based on the risk of FI's involvement in predicate offences. Qualitative risk assessment builds on AML/CFT questionnaire for obliged entities; it assesses the level of compliance and efficiency that is checked directly within obliged entities. For the obliged entities that are accountable to NB, risk assessment builds on the

number of transactions and previous violations.

932. The risks of each obliged entity are revised at least annually based on regular reports, surveys, findings of examinations and identified violations. Both ARDFM and NB have provided specific examples of increasing and decreasing the risk level initially assigned to the supervised obliged entities.

933. Also, the risk-based approach includes a reasoned judgement formed on the basis of a quantitative and qualitative analysis of the activities of the supervised obliged entities in general. This analysis includes an analysis of AML/CFT risk management and internal controls. At the time of the on-site mission, a reasoned judgement regarding risk management and internal AML/CFT control systems had not been used in practice, that does not allow the Assessment team to conclude on the effectiveness of this tool.

934. The FIs that are supervised by ARDFM are divided into four risk categories: low, medium, above medium and high. The FIs supervised by NB are divided into three categories: low, medium and high. Currently, the majority of the FIs supervised by both ARDFM and NB have medium or above medium risk levels, but there are also high and low risk FIs. Assignment of medium and low risks to the non-banking FIs, in particular, stems from the fact that they only provide services to their customers if they open accounts with STBs, that mitigates the ML/TF risk for non-banking FIs, according to the supervisors. From the assessors' view, this approach does not fully reflect the individual risk of each FI.

Table 3.4. Obliged entities' risk levels (at the time of on-site mission)

Obliged entity	High	Above medium	Medium	Low
STBs	-	15	7	-
EECTBO	-	-	-	6
Insurance companies and brokers	-	1	26	9
Security market participants	-	5	17	-
EEMA	15	7	88	920
PSP				
AI	156		126	17
Commodities exchanges	-	-	-	16
FIs of AFSA	3	-	31	4

935. ARDFM takes supervisory measures in accordance with the annual Supervision Action Plan. Based on the results of the risk assessment of the FIs, including ML/TF risk, those to be included in the plan of on-site inspections are determined. The FIs that are subject to unannounced on-site or documentary audits are also identified.

936. Frequency and duration of scheduled inspections and their coverage and the number of inspectors and the volume of transactions for checking depend on the risk level assigned to FIs. In accordance with the approved procedure, ARDFM examines above average risk STBs, security traders, insurance companies and organizations that conduct microfinance activities annually, medium risk STBs, security traders and organizations that conduct microfinance activities once per two years (medium risk CO once per three year), and low risk STBs, security traders and organizations that conduct microfinance activities one per three years (once per five years in respect of low risk CO). According to the Assessment team, the minimum frequency of inspections, especially for high-risk and above-medium risk FIs, ensures that high-risk FIs are inspected frequently enough. At the same time, given the average length of the supervisory cycle, the maximum period of 1 to 3 years in between scheduled inspections, as set out in the methodology, seems short enough to allow the supervisor to adequately review AML/CFT systems and identify breaches, as well as it does not provide FI with enough time to remedy breaches and take a follow-up control. As per existing legislation, an inspection of FIs cannot last longer than three months, which also represents a limitation of the risk-based approach. However, from the supervisors view, this requirement does not affect the effectiveness of the inspections in practice, including taking into account that ARDFM appointed its representatives in all STBs and they carried out ongoing desk based supervision. According to the information provided to the Assessment team, since 2018 and as of the on-site mission ARDFM has conducted scheduled inspections covering most of the supervised FIs, including high, medium and low risk

FIs..

937. ARDFM has sufficient resources to supervise the obliged entities' compliance with the AML/CFT requirements (67 officials supervise bank institutions, 121 officials supervise organizations that conduct microfinance activities, 40 officials supervise security traders and 50 officials supervise the insurance sector).

938. On a semi-annual basis NB includes in the list of the obliged entities to be examined the highest (high, medium and above medium) risk level entities, which enables NB to focus its control and supervisory resources on the entities of the reporting sector that are mostly exposed to ML/TF risks. In respect of low risk obliged entities, draw up a list of the obliged entities to be examined, period from the last inspection is taken into account; the selection of obliged entities is adjusted accordingly. In practice, this approach enables to include in the examination sheet low risk obliged entites. For instance, during the period under review NB twice inspected above medium risk payment institutions, 4 medium risk payment institutions and 3 low risk payment institutions; they account for 93% of the payment services market. Also, NB has sufficient resources to conduct supervision.

939. ARDFM and NB also conduct desk-based examinations of obliged entities when they identify indications of violations of legal requirements in the process of analysis of administrative data, or in connection with requests from individuals, legal entities and state bodies and other information requiring verification of compliance with the legislation, including AML/CFT legislation (see Table 3.6). From the Assessment team's view, the number of desk-based examinations in analyzed period is consistent with the risk profile of the financial sector in Kazakhstan.

940. Supervisory authorities generally conduct comprehensive supervisory inspections, during which, apart from prudential supervision, implementation of the requirements of AML/CFT laws is examined. In some cases, random AML/CFT inspections (upon FMA's requests) were conducted; also, in 2020 ARDFM conducted thematic inspections (thematic AML/CFT off-site examinations of all STBs, security market participants and insurance companies were conducted).

941. ARDFM has not fully demonstrated that it conducts consolidated supervision of compliance with AML/CFT requirements and management of international financial group's risks. ARDFM, as a supervisory authority of the parent company, has not sent requests to foreign supervisory authorities to take supervisory measures to the subsidiaries or obtain other information on the subsidiaries' compliance with AML/CFT requirements. This is due to the fact that the cooperation treaties with foreign supervisory authorities came into force relatively recently. At the same time, the ARDFM requests the necessary information on the financial group's compliance with AML/CFT requirements from its parent entity. Also, ARDFM does not take into account the subsidiaries' ML/TF risks to assess the international financial group's risks. It is worth noting that the ARDFM is the supervisory authority at the parent company level for only two STBs.

942. In respect of commodities exchanges, there exists methodology of calculation of risk levels depending on subjective and objective criteria. Inspection sheet are drawn up giving priority to the highest risk obliged entities under subjective criteria. Currently, all commodity exchanges are assigned with a low risk and from July to August 2022 the APDC inspected one commodity exchange, including AML/CFT matters, which did not result in any violations. In addition to this inspection, the APDC conducts a remote professional control, which also includes issues on compliance with AML/CFT requirements by commodity exchanges. APDC has sufficient resources to conduct supervision given low risk of supervised obliged entities (unit that comprises 5 officials, including senior officials, conducts supervision, as well as 6 officials in territorial departments of APDC in each region).

943. The AFSA has demonstrated its own good model of risk-based approach (including ML/TF risks) to inspections of AIFC members (FIs, DNFBPs and VASPs). It should be noted that the function of control and supervision of AIFC members is assigned to the AFSA in 2017 and AML/CFT control – in July 2022.

944. AFSA has developed a model to prioritize on-site inspections based on the existing individual risks

of FIs, taking into account quantitative and qualitative criteria. AFSA annually approves Comprehensive Inspection Plan that includes AML/CFT issues. Unscheduled thematic inspections are also conducted. However, due to a fairly recent introduction it is difficult to assess the efficiency of this model during the period under review. In 2020, due to COVID-19 AFSA conducted one on-site inspection of the member of AFSA that has license to conduct financial activities from 2018, which has not identified any grave violations.

Table 3.5. AML/CFT and comprehensive inspections as of 1 June, 2022

		AML/CFT inspections					**AML/CFT on-site inspections**									
							Scheduled inspections					**unscheduled inspections**				
		2018	2019	2020	2021	First half of 2022	2018	2019	2020	2021	First half of 2022	2018	2019	2020	2021	First half of 2022
ARDFM	STBs	16	20	20	36	29	7	7	2	1	4	0	0	0	4	1
	EECTBO	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0
	Insurance companies	10	4	40	4	2	10	4		10	4	0	0	0	0	0
	Securities market participants	3	5	21	1	0	3	5	0	1	0	0	0	0	0	0
	EEMA															
	MFOs	38	31	87	10	5	38	31	24	8	3	0	0	0	63	0
	Pawnshops	0	0	534	0	0	0	0	0	0	0	0	0	181	0	0
	Credit partnerships	0	0	0	2	0	0	0	2	0	0	0	0	0	0	0
NB	PSPs	6	6	11	13	8	4	3	1	0	3	0	0	0	0	0
	AIs	205	205	139	165	381	203	204	139			25	10	70		
APDC	Commodity exchanges	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AFSA		0	0	3 58 obliged entities are under AML/CFT thematic inspections												

Table 3.6. Documentary examinations and other forms of control

		AML/documentary examinations					**Other forms of control**				
		2018	**2019**	**2020**	**2021**	**First half of 2022**	**2018**	**2019**	**2020**	**2021**	**First half of 2022**
ARDFM	STBs	9	13	18	31	24					
	EECTBO	0	0	0	0	0					
	Insurance companies	0	0	40	0	0					
	Securities market participants	0	0	21	0	0					
	EEMA										
	MFOs	0	0	0	2	2			143		
	Pawnshops	0	0	353	0	0			130		
	Credit partnerships	0	0	0	0	0					
NB	PSPs	2	3	10	13	5					
	AIs	2	1	0							
APDC	Commodity exchanges	0	0	0	1	0					

DNFBPs and VASPs

945. Unscheduled inspections, preventive controls with visits (inspection) and without visits (monitoring) can be ordered in relation to DNFBPs.

946. Unscheduled inspections are carried out on the basis of the results of thematic inspections, appeals of state authorities on the facts of violations committed, individuals and legal entities, instructions of the criminal prosecution body in accordance with the CPC of the RK, General Prosecutor's Office, non-execution of orders to eliminate the previously revealed violations.

947. Inspections are appointed based on the degree of risk in relation to a particular subject, which is subjective. The risk in this case only partly takes into account the AML/CFT element, namely when the probability of harm to the property interests of the state is examined, taking into account the severity of the consequences.

948. The risk level criteria are a set of quantitative and qualitative indicators related to the direct activities of the subject, the specifics of sectoral development. Criteria of degree of risk for selection of an entity shall be developed by state agencies on the basis of the order of formation of the system of risk assessment.

949. Upon the results of the inspection, orders to eliminate the detected violations are drawn up without initiating administrative proceedings, and their implementation is monitored. In the case of gross violations detected as a result of preventive control with a visit, unscheduled inspections shall be ordered in accordance with the risk assessment criteria.

950. However, the degree of freedom of appointment of preventive control with a visit is limited by the preparation of regular schedules for half a year, which are mandatorily registered with the Committee on the legal statistics and special accounts (CLSSA) of the Prosecutor General's Office, the lack of possibility to both change them and to appoint an inspection in relation to one subject two half-year in a row, the threat of liability for unreasonable decision to conduct preventive control with a visit.

951. Monitoring is not required to register with the CLSSA, it is prohibited to visit the inspected entity. Upon the results of the inspection, certificates, conclusions, recommendations, etc. are drawn up without initiating administrative proceedings, but with the obligatory explanation to the subject of control of the procedure of elimination of the revealed violations.

952. The results of monitoring may be the basis for inspection.

953. During the interviews, the Assessment team were told that DNFBPs are selected for inspection according to a methodology for calculating the degree of risk, depending on objective and subjective criteria. The criteria take into account the outcome of the NRA, the results of previous inspections and a number of other quantitative and qualitative indicators. A DNFBP is included in the semi-annual inspection plan when the highest risk outcome under the subjective criteria is achieved.

954. FMA as a supervisory authority (function secured at the end of NRA 2021) demonstrated good understanding of the approach in supervision based on the risk of obliged entity. FMA has carried out extensive work to cover obliged entities, determine the risk level of obliges entities supervised in accordance with the AML/CFT Law.

955. List comprising 15,000 entities that conduct activities regulated by the AML/CFT Law has been generated. The entities has been filtered under a number of criteria, including the date of commencement of activities (material condition to apply Article 463 and Article 214 of the Administrative Offences Code); lack of notice on commencement/termination of obliged entities' activities; lack of STR/SARs; lack of notices under FM-1 form (special/law enforcement authorities) as a customer; electronic invoices for a period from the 1st quarter of 2021 (to identify the actual activities), etc.

956. Following review of the list, obliged entities that are supervised by FMA have been divided in 1H2022 into the following categories: 365 high risk obliged entities, 2,573 medium risk obliged entities and 12,572 low risk obliged entities.

Table 3.7. Information on the number of FMA supervised obliged entities by category and risk level (as of on-site mission)

Obliged entity's category	High	Medium	Low
Jewelers	104	392	3 208
Accountants	170	868	2 361
Real estate agents	79	145	3 252
Legal advisors	10	95	3 727

957. In turn, FMA identified 8 obliged entities from the high-risk group and included them in the inspection plan.

958. 150 obliged entities failed to notify about the commencement of their activities as obliged entity (hey were instructed to eliminate the identified violation) and 207 obliged entities were identified as having a potential risk of AML/CFT violations (provided clarifications).

959. In the 2nd half of 2021, FMA conducted 9 inspections. In the 1st half of 2022, there were 8 inspections, including 4 unscheduled inspections against jewelers. 14 inspections are scheduled for the 2nd half of 2022. Unscheduled inspections were conducted due to obliged entities' non-implementation of the instructions to eliminate the violations identified during preventive control.

Table 3.8. Identified violations and sanctions imposed in accordance with CAO

No.	Provision of Administrative Offences Code of the RK	Violations identified		Sanctions applied	
		2021	2022	2021	2022
1	Part 1, Article 214	6	4	Order to rectify violations	Order to rectify violations
2	Part 2, Article 214	12	12	Order to rectify violations	Order to rectify violations
3	Part 3, Article 214	6	0	Order to rectify violations	0
4	Part 3-1, Article 214	0	0	0	0
5	Part 4, Article 214	4	4	Order to rectify violations	Order to rectify violations
6	Part 5, Article 214	4	4	Order to rectify violations	Order to rectify violations
7	Part 6, Article 214	3	4	Order to rectify violations	Order to rectify violations
8	Part 7, Article 214	7	4	Order to rectify violations	Order to rectify violations
9	Part 8 , Article 214	4	4	Order to rectify violations	Order to rectify violations
10	Part 9, Article 214	3	4	Order to rectify violations	Order to rectify violations
11	Part 10, Article 214	12	8	Order to rectify violations	Order to rectify violations
12	Part 11, Article 214	3	4	Order to rectify violations	Order to rectify violations
13	Article 214-1	0	0	0	0
14	Part 3, Article 462	0	2	0	Administrative offence reports
15	Part 1, Article 463	5	4	Order to rectify violations	Order to rectify violations

960. Following the inspections conducted in 2021, 69 violations were identified, in 2022, 58 violations were identified. The violations relate to non-compliance with the AML/CFT requirements. Based on the results of the inspections, orders were issued to eliminate the identified violations within 3 months. SFM, who did not fulfil the instructions, were brought to administrative responsibility under Part 3 Article 462 (obstructing officials of state inspections and state control and supervision bodies in the performance of their duties, failure to comply with orders, instructions and other requirements) of the Administrative Code and fined from 200 MCI (approx. 1,300 USD) to 500 MCI (approx. $ 3,300 USD).

961. In respect of average and low risk entities that are accountable to FMA, the following preventive measures are taken using FMA web-portal: explanations, training events, information and notices are communicated to obliged entities through open information sources.

962. Based on the results of the remote monitoring, the FMA supervised obliged entities receive letters (notices) on the need to remedy the identified violations.

Table 3.9. Results of remote monitoring of FMA supervised obliged entities

	Leasing companies	**Jewelers**	**Real estate agents**	**Accountants**	**Legal advisors**	**Overall**
	Identified violations and their quantity					
Noticed issued	1 Lack of registration	36	50 12 – lack of registration 38 – no notification	54 Lack of registration	9 Lack of registration	150
	Result of the remedial action					
Passed through registration	1	33	5	36	9	84
Sent notification	0	0	38	0	0	38
Not addressed: on execution, discontinuation/other activities	0	3 On execution	7 3 – other activities 4 – on execution	18 2 – other activities 16 – on execution	0	28 5 – other activities 23 – on execution

963. As it follows from the information provided, according to the results of remote monitoring, there are still non addressed violations, the deadline for elimination of which has not yet arrived, or the obliged entities carry out activities that are not declared as core and are not subject to notification of the start of activities as an obliged entity. The FMA staff assigned to each category of obliged entities, conduct analysis of the elimination of identified deficiencies/violations. Therefore, the assessors concluded that FMA has a good level of supervision and monitoring of supervised obliged entities, that allows to mitigate the identified risks.

964. FMA performs the ongoing monitoring of supervised obliged entities via software of the FMA web portal, as well as other data the FMA has access to. The inspection plan is adjusted either at the decision of the FMA or due to change of the records of supervised obliged entities or indicators, which are the basis of forming the plan initially.

965. FMA has 5 employees that conduct inspections, at least 2 employees are appointed for each inspection. This number seems sufficient in view of the focus on prevention in FMA's supervisory activities.

966. It should be noted that the capabilities of SRBs (for instance, real estate association) are insufficiently employed to conduct inspections. This may relate, inter alia, to the low involvement of this category of obliged entities in the SRB’s activities.

967. The risk assessment of the obliged entities supervised by the MCS, is based on the results of NRAs conducted in 2018 and 2021, as well as the results of quantitative and qualitative indicators, including the results of monitoring of quarterly reports of organizer of gambling industry; results of analysis of information received from state authorities, results of past inspections and monitoring, availability of complaints, etc.

968. The risk level of the obliged entities is reviewed on a quarterly basis as part of monitoring, and this results in a semi-annual inspection plan.

Table 3.10. Information on the number of obliged entities supervised by the MCS, ordered by category and risk level (at the time of the field mission)

Obliged entities category	**High**	**Medium**	**Low**
Casinos	0	0	6

Gaming machine halls	0	4	7
Bookmaker offices	1	18	10
Totalizators	0	5	2

969. Unscheduled inspection of 1 obliged entity in 2018, preventive control with visits to 2 entities in 2019, and 1 entity in 2022. AML/CFT violations have not been identified. In 2020-2021, control measures, including on AML/CFT matters, were not conducted due to the introduced quarantine measures.

970. The MCS has 2 divisions with control functions and a staff of 8 persons, who can be involved in the inspections. In addition, the relevant association provides reporting, that is the basis for MCS monitoring of implementation of AML/CFT obligations as well. The MCS considers that this number of inspectors is sufficient for 2 gaming zones, to which the experts agreed.

971. Assessors note active involvement of MCS in joint inspections along with the General Prosecutor's Office and Economic Investigation Service of FMA. 4 these inspections are scheduled for 2022.

972. In addition, the MCS, in cooperation with MISD, the Service of economic investigations of FMA, the Prosecutor General's Office and the Ministry of Interior, identify and block online casino sites whose activities are prohibited in the country which corresponds to the risks identified in the NRA-2021. For this purpose, the country uses the "Kibernadzor" information system, which is filled with links to online resources containing such illegal content. In 2018, the 165pprox.165in body issued 28 prescriptions to restrict the distribution of materials with indications of Internet casino activity and advertising in relation to 420 illegal materials (Internet resources and links) entered into the Kibernadzor IS; in 2019 – 36 prescriptions in relation to 659 materials; in 2020 – 21 prescriptions in relation to 252 materials; in 2021 – 62 prescriptions in relation to 2 618 materials; in 2022 – 147 prescriptions in relation to 5 5 511 materials. All the prescriptions are being fulfilled.

973. Based on the results of the ML/TF NRA 2018, the audit organisations were classified as high risk, which is why the IPAC has taken some measures to implement a risk-based approach in its oversight.

974. IPAC along with FMA has developed a risk management system according to which audit firms that are not subject to mandatory audit are also classified as high risk.

975. A joint order of the First Deputy Prime Minister – Minister of Finance of the RK dated 15.07.2019 No. 724 and the Minister of National Economy of the RK dated 16.07.2019 No. 65 "On Approval of Risk Assessment Criteria and Checklists in Audit Activities" was also developed, which provides for two AML/CFT-related items as subjective criteria (compliance with internal controls, interaction with FMA).

976. In addition, as part of listing the entities for inspection, IPAC continuously analyses the reports submitted by the supervised obliged entities, information from other state authorities, and applications from individuals and legal entities as subjective criteria.

977. In 2018-2020, no audit firm was assigned a high risk level. In 2021, 4 audit firms were classified as high risk and were subject to inspections, with another 1 firm subject to an unscheduled inspection. In 2022, 19 audit firms were classified as high risk, of which 2 were inspected at the time of the on-site mission. No AML/CFT violations were identified. The increase in the number of high-risk audit firms may indicate an increased understanding of risk in the sector by IPAC to some extent.

978. Relevant SRBs conduct documentary examinations of audit firms at least once per 3 years as part of quality control. The outcomes of this work may serve as grounds to conduct an unscheduled inspection. However, there are no such examples. Assessment team have concluded that such monitoring is not sufficiently effective.

979. IPAC has an appropriate unit with control functions that comprises 7 officials. Regional departments of IPAC, where these functions are exercised by financial report units with a staff of 60 officials, also conduct inspections. The assessment team concluded that this number is sufficient to cover the supervised obliged entities with inspections.

980. To assign risk levels to the controlled entities that conduct notaries' activities, Ministry of Justice uses Criteria of risk level assessment and inspection sheet with respect to notaries' activities.

981. In order to select notary for the inspection MoJ investigates the existence of a fact of bringing the subject of control to disciplinary or administrative responsibility during the year; failure of notary to provide to FMA information and data on transactions subject to financial monitoring; failure of notary to provide within a month to the territorial justice body information on changes in his name, surname, patronymic, as well as the location of his office; existence of a fact of suspension of the license for notarial activity.

982. In the light of the application of the MoJ's risk system, lists of entities to be inspected are drawn up on semi-annual basis. Should there is a high risk, a notary may be included in the list of inspections 2 times per year. In the analysed period 556 high-risk notaries were inspected.

983. In the Republic of Kazakhstan, 28 officials conduct inspections of notaries.

Table 3.11. Statistics of control activities carried out by the MoJ in relation to notaries

	2018	2019	2020	2021	I half of 2022
Preventive control with visits	14	189	104	164	78
Unscheduled inspections	220	252	214	561	247
Preventive control without visits	-	-	9	21	16

984. As can be seen from the data provided, the main focus of the MoJ's supervisory activities is on inspections. There are up to 19 inspections per inspector per year. All of the notary's documents are subject to inspection. There is almost no use of monitoring activities and no involvement of SRBs in this part.

985. The National Bar Association will be required to monitor and analyse the work of advocates through the territorial chambers of advocates. In view of the entry into force of the relevant amendments only from 01.09.2022, no such inspections have yet been carried out in practice.

986. The model for assigning on-site inspections of DNFBPs and VASPs in AIFC is the same as for FIs in AIFC. In addition, the AFSA examines regular reporting and the results of previous inspections as part of ongoing monitoring, using software tools to carry out daily supervision. Also for the purpose of thematic inspections, the AFSA has developed a special questionnaire with 11 sections and 135 questions concerning the components of the subject's ML/TF risk control system. The subject must provide supporting documents and references to its policies and procedures to the answers The AML/CFT risk rating of the subject of financial monitoring in AIFC is assigned taking into account the definition of the risk environment and the assessment of the controls in place. In turn, each control also has a scoring system. All of the obliged entities in AIFC – DNFBPs and VASPs – have an average risk.

987. Such practice of continuous monitoring allows the AFSA to receive timely information on the current status of both the individual obliged entities and the sector as a whole, as well as to plan follow-up supervisory activities.

988. At the time of the on-site mission 2 VASPs are under on-site thematic inspections. Full inspection cycle in relation to these VASPs have not been completed yet as of on-site mission.

989. When MDD conducts inspections, it follows the requirements of the COMC of the RK. Due to the fact that at the time of the on-site mission the obliged entities have not submitted notices of commencement of their activities, this Ministry has not conducted these inspections.

6.2.4. Corrective measures and effective, proportionate and dissuasive sanctions

990. In general, supervisory authorities apply a wide range of corrective measures when checking compliance with AML/CFT requirements, but the statistics provided and the existing system of imposing administrative fines do not allow to conclude that these measures are proportionate to the violations committed and are sufficiently effective to prevent further violations of AML/CFT legislation in other obliged entities.

991. All supervisory authorities have the right to apply corrective measures and sanctions to the supervised obliged entities for violations of AML/CFT requirements. At the same time, administrative fines for AML/CTF violations shall be imposed by not the supervisory authorities, but the courts on the basis of reports of supervisory authorities. The administrative fines may not be imposed on officials of the obliged entities, that are not quasi-public entities. In such a case the officials may be held liable by way of recourse, and other corrective measures may be applied to them. The exception is Article 214-1 of the CAO, which was enacted in July 2022, and there is no practice of its application as of on-site mission.

992. Fines are imposed on the obliged entities by drawing up reports by the supervisory authority for each individual breach and submitting them to the court. In practice, judges may combine reports against one obliged entity in one proceeding and impose a maximum fine of 6000 MCIs (1 MCI is equal to 3,180 KZT or ~6.65 USD at the time of on-site mission). In some cases reports against one obliged entity were distributed among several judges, who, in turn, combined them and each time appointed the maximum fines.

993. This practice of applying measures and penalties to the obliged entities shows that they are not proportionate.

994. Supervisory authorities have the right to take measures of supervisory response for violations of AML/CFT requirements, including revocation of the license, prescriptions, experienced judgment, suspension of a manager from his duties, and are required to submit protocols for the imposition of administrative fines for AML/CFT law violations as prescribed in the CAO to the court. At the same time, they may not apply corrective measures instead of drawing up breach reports to send to the court and impose fines because, in accordance with Article 806 of the Code of Administrative Offences, an administrative offence report is drawn up immediately after the discovery of an administrative offence.

995. According to the Assessment team, this approach does not allow for the full application of corrective measures proportionate to the violations detected, as the supervisory authority has no possibility not to apply an administrative fine or to adapt the amount of the fine to the specific situation of the obliged entity. At the same time, such an approach, which limits the discretion of the oversight bodies, is explained in the Kazakhstan by the combating on corruption.

Financial institutions

996. In the assessed period, the supervisory authorities (ARDFM and NB) mainly drew up reports for imposing fines for identified AML/CFT breaches, as well as issued instructions to eliminate them. The main breaches concerned the lack of internal control rules, inadequate internal control rules, inadequate customer identification program, failure to provide notifications to the FMA on threshold or suspicious transactions as well as on freezing measures, inadequate automated systems for detecting threshold, unusual and suspicious transactions, violation of time limits for notifying the FMA, failure to comply with requirements regarding training programs.

Table 3.12. Statistics of detected breaches of FIs (number of reports by type of breach)

	2018			**2019**			**2020**			**2021**			**6 months of 2022**		
STBs	25			19			740			81			3		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	2	18	5	1	17	1	5	121	64	1	71	9	0	0	1
EECTBO	0			0			0			0			0		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Insurance companies	62			14			38			0			0		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	6	56	0	2	12	0	3	35	3	0	0	0	0	0	0
Securities	460			77			4			-			-		

market participants															
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	1	459	0	2	75	0	4	0	0	0	0	0	0	0	0
EEMA	28			12			51			-			4		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	25	3	0	8	4	0	28	23	0	0	0	0	1	3	0
PSP															
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
AI	69			480			134			44			0		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other
	0	13	56	0	15	465	0	47	87	2	5	37			
Commodity exchanges	0			0			0			14			0		
Type of breach	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ICR	STR	Other	ПВК	STR	Other
	0	0	0	0	0	0	0	0	0	14	0	0	0	0	0
AIFC	0			0			0			0			0		

997. In the period under analysis, the ARDFM and NB did not revoke licenses for AML/CFT breaches due to the absence of a pattern of systematic violations of AML/CFT legislation by obliged entities, in the opinion of the supervisors. Also, the ARDFM did not apply the tool of experienced judgment to the effectiveness of the risk management and internal controls of the obliged entities in the AML/CFT sphere, but only to the impeccable business reputation of senior managers. Thus, the person in respect of whom the supervisory authority withdrew consent for the appointment to the position of executive officer – Chairman of the Management Board of the Insurance Organisation – in 2017 has submitted documents for approval for the appointment to an executive officer position at the obliged entity. The issue of refusal of approval has now been submitted to the ARDFM for consideration in the framework of a reasoned judgement.

998. During the analyzed period, the FMA made 75 submissions to the STBs to eliminate the circumstances that contributed to the criminal offence and other violations of the AML/CFT regulations. These submissions mainly concerned the failure to suspend suspicious transactions prior to their execution, which in the opinion of the assessment team is consistent with the risk profile of these FIs and the shortcomings of the internal procedures identified by the ARDFM (see Chapter 5).

999. The statistics in Table 3.12 demonstrate that the number of detected violations of AML/CFT legislation has decreased in all sectors, which indicates the effectiveness of supervisory measures aimed at one-time correction of documentation deficiencies and an improved understanding of FIs' responsibilities in this area, according to the Assessment team. The effectiveness of the corrective measures and sanctions applied is confirmed in each individual case of breaches committed by the obliged entities, since in most cases no instances of repeated breaches are found. At the same time, there is no identified trend of lower non-sending or untimely sending of STRs for all sectors, as well as other AML/CFT violations, indicating a lack of effectiveness of the supervisory measures taken. The lack of identified STR violations in most sectors in 2021 is due to the absence or low number of on-site inspections conducted.

Case Study 3.3

In 2021, the subsidiary Islamic “Al Hilal” bank was fined for failure to provide information on transactions that are subject to financial monitoring in a timely manner. The reason for this was the announcement of an additional day off for bank officers by the parent company (shareholder), during which transactions that are subject to financial monitoring were conducted. The Bank identified and corrected the deficiency, but a fine was imposed for each failed transaction. As a consequence, the Bank’s ICR was supplemented with a quarterly review of all transactions for the period against transactions

reported to the FMA.

Case study 3.4

During the period under review, the FMSA found violations of AML/CFT legislation on suspicious transactions in several STBs, including failure to report transactions and failure to suspend transactions despite indications of suspicion. The recommendations were followed by disciplinary proceedings against 7 employees of these second-tier banks (*2 in 2018, 1 in 2019, 2 in 2021, and 2 in 2022*) and the dismissal of 3 employees (1 each in 2020, 2021, and 2022). The rest of the submissions were explained and the employees of STB were trained.

1000. No corrective measures and sanctions were applied to the obliged entities controlled by the AFSA during the analyzed period, as no serious violations were identified due to the lack of completed inspections for most of the FIs in AIFC, that does not allow to conclude about the effectiveness of sanctions and supervisory response measures. However, it is worth noting that the AFSA is currently investigating 12 AML/CFT breaches identified during the inspections conducted in 2022 after on-site mission.

1001. Due to the fact that the body authorized to process cases of administrative breaches by commodity exchanges is the Ministry of Trade and Integration of the Republic of Kazakhstan (MTI), the relevant materials on breaches identified in 2021 were submitted by the APDC to the MTI. Based on the results of consideration of administrative cases, 3 commodity exchanges were brought to administrative liability.

1002. All corrective and sanction measures are of a public nature and may cause reputational damage to the obliged entities to which they are applied. Thus, they have a certain dissuasive effect on some obliged entities, as evidenced by the information provided by them.

1003. At the same time, the information and statistics provided do not allow for an unambiguous conclusion of the assessment team that sanctions are proportionate and have a deterrent effect on the prevention of AML/CFT legislation violations in general. According to interviewed FIs, the level of fines imposed is high and even in some cases too high for small FIs, but the system of imposing fines does not always lead to a consistent result and the total amount of fines imposed may be different for the same violations (see par 993). Thus, according to statistics provided by CLSSA, there were 548 administrative cases under Article 214 of the CAO in 2018, 586 in 2019, 108 in 2020 and 110 in 2021, which may indicate a decrease in the number of violations. At the same time, according to the information provided by the FMA, the number of submissions to eliminate the circumstances contributing to the commission of a criminal offence and other violations of the law, as well as those related to violations of AML/CFT requirements, on the contrary, has increased.

Table 3.13. Statistics on FMA's supervisory submissions

	STBs	NB	ARDFM
2018	2	2	-
2019	5	1	-
2020	28	1	1
2021	31	5	13
6 months of 2022	9	-	-

DNFBPs and VASPs

1004. As a result of control measures carried out by FMA revealed violations of AML/CFT legislation, as well as violations related to engaging in business or other activities, carrying out actions (operations) without appropriate registration, authorisation or notification. 31 prescriptions to eliminate revealed violations were issued. 26 prescriptions were executed in timely manner. Five administrative reports were drawn up for failure to comply with the prescriptions, resulting in fines of 3,981,900 KZT (~$ 8,500).

1005. The MoJ's verification activities (see Table 3.11) identified irregularities related to late notification of a suspicious transaction.

Table 3.14. Statistics on the number of violations detected as a result of inspections of notaries and the measures taken against notaries in the form of administrative liability (AL) and the amount of fines

	2018	2019	2020	2021	1 пол 2022
Violations detected	2	18	36	23	17
Notaries took AL	2	18	36	23	17
fines applied, KZT	1 193 359	6 812 459	9 726 465	2 730 312	2 087 520
Eq. USD	1 768	16 323	24 064	6 215	4 488

Note: USD equivalent is based on the exchange rate for the respective year.

1006. It follows from the statistics presented that the penalties imposed have no impact on the overall downward trend in the number of AML/CFT violations detected and are, therefore, not deterrent. The provided statistics for notaries demonstrates a sharp increase in violations in 2020 and a relatively slight decrease in 2021. The amounts of fines per violation vary from 596,7 thousand KZT in 2018 to 118,7 thousand KZT in 2021. With a substantial reduction in the amount of fines, the reduction in the number of violations was insignificant.

1007. As mentioned above, the MCS and IPAC also conducted AML/CFT inspections and identified no violations. However, due to AML/CFT violations both audit firms and organizers of gambling industry were recognized as risky in NRA-2018 and NRA-2021 respectively. Thus, these circumstances may indicate a lack of attention to AML/CFT issues in the course of inspections.

1008. It is worth noting that other measures, such as suspension, termination or withdrawal of licence, are also applied in the country (see Tables 3.1-3.3).

1009. Based on the information provided on the forms of corrective measures and fines imposed on the obliged entities, it appears that these measures are not diverse, do not have a decreasing trend in the number of identified AML/CFT violations, are therefore not dissuasive and, therefore, are not fully effective. It appears that one of the factors reducing the effectiveness of the application of penalties is the lack of possibility of supervisors to apply measures of administrative liability and to hold the officials of obliged entities administratively liable (see analysis R.35).

1010. It should be noted that the work of supervisory authorities is aimed at preventing the commission of AML/CFT violations. The awareness-raising activities: trainings, working meetings, drafting memos, recommendations, etc, are conducted to achieve this. FMA plays a special role in this area, as well as significant work is carried out by respective SRBs.

1011. The AIFC law establishes a wide range of corrective actions and sanctions: instruction to take corrective action on identified deficiencies within a specified time frame, fines, license limitation (suspension, partial suspension, revocation), prohibition on certain operations, censure, restriction, suspension, revocation of managerial status, deprivation of the obliged entity employee, forced appointment of a temporary manager, involuntary termination of operations, restitution order, public notice, private warning, etc.

1012. Sanctions apply to the VASP official who committed the breach.

1013. When imposing a sanction (a fine or other corrective measure), the AFSA proceeds from the breach seriousness, the presence of intent and an assessment of the consequences of the act committed.

1014. If at any stage of the inspection there are clear indicators of a criminal offence, the information is transferred to the relevant authorized body of the Republic of Kazakhstan. At the same time, the investigation of breaches within the AFSA's purview may continue.

1015. However, it should be noted that the inspections of VASPs and DNFBPs in AIFC were not completed up to the determination (assignment) of corrective measures at the time of the on-site mission, therefore the

effectiveness in this part was not assessed.

6.2.5. Impact of measures taken by the supervisory authorities on compliance with AML/CFT requirements

Financial institutions

1016. The impact of supervisory measures on AML/CFT compliance varies across requirements and sectors.

1017. With respect to the obliged entities supervised by the ARDFM and NB, when breaches of AML/CFT compliance requirements are identified, along with the imposition of fines, a plan to eliminate the breaches is prepared jointly with the obliged entities and its implementation is monitored by the supervisory authority. According to the ARDFM and NB, the violations identified are remedied by the FIs in a timely manner (from a month to a year, depending on the nature of the violation) and are not detected repeatedly. There are also examples of the application of recommendatory measures by the ARDFM aimed at improving the internal control systems of the obliged entities, not related to the breach of AML/CFT legislation, such as increasing the number of employees, automation of STRs submission, readjustment of client risk assessment parameters which has a positive impact on compliance with AML/CFT requirements by supervised FIs, according to supervisory authorities and FIs interviewed. The substantial decrease in the number of violations of AML/CFT legislation in the analyzed period confirms this conclusion. However, the supervisory authorities lack a systematic approach to assessing the impact of measures taken and general indicators of improvements in AML/CFT compliance by the obliged entities.

1018. The APDC sent recommendations to correct the identified breaches based on the results of the off-site professional inspection in 2021-2022. Based on the information provided to the assessors, the commodity exchanges informed the APDC in writing about the full implementation of the recommendations. The remediation of the previously identified violations is also verified by the APDC on an ongoing basis, through monitoring of internet resources and other sources of information on a quarterly basis.

Case Study 3.5

In practice, case studies provided by supervisors show that the obliged entities are implementing the action plan and eliminating the identified breaches, as well as improving internal control systems according to the recommendations received.

For example, in 2022, the ARDFM issued an order against Jusan Bank requiring the replacement of the internal control team for systematic non-compliance with the AML/CFT requirements for suspicious transactions reporting. The bank complied with the supervisory authority's request by completely replacing the compliance team.

1019. Regarding FIs in AIFC, the AFSA recommended one of the obliged entities to correct deficiencies in internal documentation identified during the 2020 online audit, and the deficiencies have been corrected. Also, there is a trial period for FIs in AIFC before starting operations, during which the obliged entities must eliminate any identified internal control deficiencies.

DNFBPs and VASPs

1020. The information and statistics provided indicate that the breaches being detected are not serious, given the business specifics of individual categories of DNFBPs. Ongoing interaction between the supervisory authorities and the obliged entities (monitoring activities, analysis of periodic reporting, call centre established in the FMA for ongoing interaction, etc.), along with lack of inspections in individual sectors (e.g., the MCS did not conduct inspections in 2020-2021 due to COVID-19 pandemic) suggests a moderate level of impact of measures on the sector of DNFBPs generally in the country.

1021. However, representatives of DNFBPs with whom the assessment team met during the on-site mission

noted the positive impact of the supervisory activities, and even more so the impact of the 2018 and 2021 ML and TF/PF NRAs. By following the supervisors' guidance and recommendations and filling out the NRA questionnaires, they became more aware of their AML/CFT obligations.

Case study 3.6

In the first half of 2021, "AK" (jewelers) was included in the preventive control inspection plan due to a high ML/TF risk. An inspection was carried out in the second half of 2021 and 12 recommendations to eliminate deficiencies were issued based on its results.

"AK" has carried out work and this company has submitted a notification to start operating as an obliged entity and registered in the Personal Account, internal control rules have been developed, taking into account the approved 5 programmes, STRs are identified and sent, and "AK" is an active participant in the Compliance Council.

In addition, more than 10 jewelers, following the sanctions imposed on "AK", have independently sent notifications on starting activities as an obliged entity to FMA and started to build their internal control systems.

1022. The supervisory authorities have demonstrated a number of performance indicators for supervised obliged entities, indicating the impact of supervisory measures on AML/CFT compliance, relating mainly to the number of STRs sent, the increase in the number of obliged entities that have submitted notifications to commence operations. At the same time, supervisors, with the exception of FMA, have no systematic approach to assessing the impact of the measures taken and no indicators of improvements in AML/CFT compliance by obliged entities.

1023. When violations are detected during inspections, MoJ issues prescriptions for eliminating the identified violations, indicating respective deadline. In the event of non-compliance with the prescriptions, they apply harsher penalties, such as measure of administrative liability. No violations of AML/CFT legislation have been identified by the MCS and IPAC, but should they are identified, the procedure for monitoring the implementation of the prescriptions is the same here.

1024. In order to determine the impact of the measures taken, the supervisory authorities analyse regular departmental statistics.

1025. The "Personal Account" on the FMA web portal plays a major role in this work. Using the capabilities of the "Personal Account", identified violations in internal control systems are promptly eliminated, including adjustments to the necessary documents. As a result of this work, no violations are identified in such areas as the obligation to apply TFS and the completion of training, which has a positive impact on the effectiveness of AML/CFT compliance.

1026. Within the inspections of AIFC members (DNFBPs and VASPs), the final stage is the drawing up of a corrective action plan by the AFSA as well as follow-up reports on the execution of the planned actions. A designated staff of AFSA monitors implementation of the plan. The risk profile of the entity is updated upon completion of the inspection cycle, and information on inspection is included in the annual report of the AIFC Board. Copies of the reports and plans are kept in the entity's file. At the time of on-site mission, there were no completed inspections up to identification and imposition of sanctions on AIFC member, so it was not possible to assess the impact of the measures taken by the AFSA.

6.2.6. Facilitating a clear understanding of AML/CFT obligations and ML/TF risks

1027. Supervisors, in particular FMA, have made significant efforts in the analyzed period to improve the understanding of AML/CFT obligations and ML/TF risks by the obliged entities, and use a wide range of measures to engage with the supervised obliged entities.

1028. The FMA's extensive work for the FIs and DNFBPs and VASPs and other supervisors is effective.

1029. The FMA has created and constantly improves its own web portal (website) on the Internet and online

services therein. The FMA web portal contains up-to-date materials, including NRA summaries, ML/TF charts and typologies. FMA develops a telegram channel (around 6 thousand subscribers). Also, there is so-called "mentoring" (assignment of a responsible staff to each category of obliged entities) in FMA.

1030. FMA's training during and following the NRA process also contributed to strengthening and understanding of ML/TF threats, vulnerabilities and risks.

1031. One of the important areas of the FMA's efforts aimed at enhancing the understanding of the obliged entities' AML/CFT obligations to increase the coverage of the obliged entities involved in this area. Thus, in 2021, 1,463 of the obliged entities registered for the first time in the Financial Transaction Data Collection System (FTDC), which is 3.5 times more than was recorded in 2020.

1032. As part of enhancing the interaction between the FMA and the obliged entities and supervisory authorities, one of the components of the FMA portal – the online service "Personal Account" – was introduced. This online service provides advanced functionality, including the capability to generate and submit STR/SARs, as well as the following categories:

- personal data (necessary information on the obliged entities, availability and assessment of ICR, passing the test), work with the TF-related List (viewing, downloading, notification), where 7 thousand of the obliged entities have updated their information in 2021;
- work with the TF-related List (viewing, downloading and notification) – 16 thousand downloads in 2021;
- training of the obliged entities (AML/CFT legislation, recommendations, memos, policy briefs, description of typologies, etc.) – more than 3 thousand downloads in 2021;
- publication of reporting data (STR/SARs, coverage of the obliged entities, involvement, etc.);
- feedback (implementation of this category allowed to reduce document flow by 2 thousand reports in 2021);
- total traffic – more than 60 thousand visits in 2021.

1033. As for typologies, it should be noted that they were developed jointly by officers of the FMA, government authorities and compliance services. The List contains 57 typologies published in 2017-2022. The typologies concern each type of the obliged entities, indicating the predicate offence for ML, e.g. illicit drug trafficking, illegal activities, embezzlement of public funds. This list includes both general typologies, which can be used by the obliged entities at a certain stage of transactions and financial operations with property, and specific typologies intended for a certain category of the obliged entities or related to a certain financial instrument, such as digital assets.

1034. Besides that, each of the obliged entities is ranked according to the rating, which is presented in the "Personal Account". This tool is designed to reflect the general level of understanding by the obliged entities of their obligations. The activity of the obliged entities on the FMA portal, consultations, study of awareness-raising and training materials are taken into account when assigning the final ranking, which promotes the activity of the obliged entities and further its awareness of AML/CFT issues and improvement of understanding and fulfillment of obligations.

Case Study 3.7 (procedure for assessing the activity of the obliged entities)

The assessment is carried out according to 6 criteria: availability of general data, compliance, actions, qualification, availability of regulatory documents, financial monitoring operations. For each of the criteria a certain number of points is awarded, depending on the compliance of the entities with the following criteria:

"General data": filling in the personal profile of the obliged entity, education and presence/absence of criminal record of the beneficiary owner, senior manager, the obliged entities themselves;

"Compliance": absence of AML/CFT legislation breaches for a certain period;

"Regulatory documents": availability of relevant internal control rules and risk management system in the entity's personal account;

"Financial monitoring operations": the activity of the entity in terms of sending reports on suspicious and threshold operations and reports with the type of Typology or ICR measure (according to special form FM-1);

"Qualification": availability of certificates of passing the AML/CFT law test, viewing the training materials on the Agency's website;

"Actions": visits to the FMA portal, completion of the FMA feedback questionnaire.

The STBs are assessed according to the following five indicators:

1) Level of STBs' interaction with the FMA;

2) Quality of suspension of transactions;

3) Correctness of submitted reports;

4) Application of "internal control rules";

5) Interaction of STBs with risk persons.

1035. One of the ways to increase understanding of AML/CFT obligations by the obliged entities is to subscribe to "FMA Channel" in the "Telegram" messenger. It publishes the latest news and successful case investigations, etc.

1036. The involvement of the obliged entities in participation in professional groups in messengers has a great influence on the understanding of AML/CFT obligations.

1037. The FMA has an always active "Hotline" that allows a compliance officer of any type of the obliged entities and a government authority representative to call a short number for qualified advice or clarification on AML/CFT issues.

1038. The FMA has also established a Compliance Council. It is composed of specialists from government authorities and certain types of the obliged entities. The Compliance Council regularly discusses current issues to improve AML/CFT internal controls.

Case Study 3.8 (Compliance Council)

The AML/CFT Compliance Council was established in November 2019 as a discussion platform for improving the quality of information exchange based on a risk-based approach between the obliged entities and the authorized body for AML/CFT financial monitoring.

The Council is chaired by the FMA Chairman; during his absence, the functions are performed by the FMA First Deputy Chairman.

Composition of the Council:

Representatives of the FMA, state regulators, public organizations and obliged entities.

Main tasks:

- Preparation of recommendations for the introduction of new formats of interaction with the obliged entities and receiving feedback;
- Preparation and discussion of proposals to improve information exchange between the obliged entities and the authorized body engaged in financial monitoring as well as other issues of information exchange;
- Participation in projects related to informing the obliged entities about ML/TF risks for practical use in implementing internal control procedures;
- Development of typologies, schemes and methods of money laundering and terrorist financing;

- Organizing and participating in joint training events, exchanging AML/CFT best practices and experience, including with the participation of experts;
- Involvement of the expert community in expert, sociological and sectoral research in the AML/CFT sphere;
- Preparation of proposals for the agendas of consultations of the obliged entities conducted by the EAG and participation in AML/CFT forums.

1039. An element of testing the knowledge of their AML/CFT obligations is defined as mandatory training and testing on its results for the obliged entities, which must take place at least once every 3 years from the date of the last test at the JSC "National Centre for Civil Service Personnel Management" and its territorial subdivisions. This site is used by the FMA for the convenience of the subjects, as this JSC has regional branches, as well as all the necessary technical equipment to conduct quality testing.

Financial institutions

1040. The FMA's efforts on enhancing the awareness of the supervisory authorities and the obliged entities of their AML/CFT obligations and risks contributes to a better understanding of AML/CFT obligations. The FMA also carries out mandatory certification of the staff of the internal control services of the obliged entities.

1041. Other supervisory authorities also conduct regular training for both their own staff and the staff of the obliged entities.

1042. The ARDFM and NB publish guidelines and typologies and provide clarifications of AML/CFT requirements for the obliged entities under their control.

1043. The ARDFM, together with the FMA, published recommendations on interacting with persons designated in the sanction list, on identifying beneficial owners and PEPs. The ARDFM also published an information document describing threshold transactions, reports on pyramid schemes and scams. The ARDFM published explanations for the obliged entities in the "question and answer" section and held a series of meetings, workshops and consultations, together with the FMA and NB on various AML/CFT issues, also involving STBs, insurance companies, professional securities market participants.

1044. The NB held a series of events and training workshops for its officers, including with international organizations, and disseminated clarifications among the obliged entities on changes in AML/CFT legislation and AML/CFT obligations of the obliged entities.

1045. The APDC did not conduct any training for its employees during the period under analysis. Regarding the regulated obliged entities, the APDC conducted a number of awareness-raising activities for commodity exchanges on AML/CFT legislation on "Customer Identification Program", "ML/TF Risk Management Program", "Clarification of the legislation in the sphere of AML/CFT" and "Understanding of risks and duties in the sphere of ML/TF", "Clarification of rules of submission of data and information on operations, subject to financial monitoring". Also, together with FMA, APDC communicated the results of the NRA to commodity exchanges.

DNFBPs and VASPs

1046. Supervisory authorities use a variety of opportunities to increase understanding of AML/CFT obligations by DNFBPs. These include regular training, outreach and prevention activities with for the obliged entities, knowledge monitoring, feedback on typologies and suspicious transactions and recommendations to correct breaches and other deficiencies identified during inspections.

Table 3.15. Statistics of training, outreach and prevention activities, workshops, courses for DNFBPs

		2018	2019	2020	2021	I half of 2022
FMA	Real estate agents	3	22	4	4	6
	Accountants	1	22	1	6	7
	Jewelers	1	23	2	5	6

	Leasing companies	1	22	1	2	6
	Legal advisors	-	22	1	2	6
MCS	Organizer of gambling industry		4	6	5	3
MoJ	Notaries, lawyers	24	31	24	44	61
IPAC	Audit firms		2	2	4	3
AIFC	DNFBPs			5	4	9
	VASPs			6	5	12

1047. A great deal of work on understanding the obligations of DNFBPs is carried out by industry SRBs. Some SRBs have developed programs and conduct regular AML/CFT training for their members (chambers of notaries, audit firms, real estate agents, accountants, jewelers).

1048. The Union of Auditors of Kazakhstan developed for its members a training workshop "Combating Money Laundering and Financing of Terrorism by Auditors of the Republic of Kazakhstan" published on its website.

1049. Professional organizations of accountants, self-regulated associations of realtors of Kazakhstan have developed memos for their members taking into account the specifics of their activities. The memos explain AML/CFT obligations, provide contacts for additional information.

1050. The RK Chamber of Notaries publishes AML/CFT training videos on youtube channel. In cooperation with the territorial bodies of justice and bar associations, it carries out explanatory work among notaries and advocates on compliance with the requirements of the AML/CFT Law. The Chamber of Notaries and territorial chambers of advocates operate professional development and training centers for notaries and advocates. Between 2017 and the first half of 2022, 227 seminars and refresher courses on AML/CFT legislation were held for notaries and 119 for lawyers. A total of 17,124 notaries and 6,984 lawyers were trained.

1051. Besides that, SRBs provide training and follow-up certifications for their members. For example, realtors, auditors, notaries are certified at the beginning of their work and thereafter, depending on the length of service. The certification questions include a sections related to understanding of AML/CFT obligations.

1052. The legal basis for the interaction between the FMA and SRBs are the signed memorandums of cooperation (professional organizations of accountants – 14 MoCs, jewelers' public associations – 2 MoCs, Association of Realtors and Chamber of Legal Advisors – 1 MoC each). These MoCs provide for carrying out work to explain AML/CFT requirements, exchange of information, joint events at the Compliance Council, dissemination of the National Risk Assessment Report, communication of legislation breaches.

1053. Supervisors work closely with the FMA and industry SRBs on improvements in the sphere of AML/CFT obligations and ML/TF risks. They also prepare various methodological guidelines, taking into account the sector's specifics.

1054. The FMA's extensive work, including for its supervised sectors, is provided in this section above. MCS has prepared methodological guidelines on identifying beneficial ownership, PEPs; 4 memos on customer identification for the purpose of reducing ML/TF risks.

1055. On April 15, 2022, the AFSA approved the AML/CFT Practice Manual for Obliged Entities, which includes an explanation of AML/CFT requirements, as well as risk indicators for business and customer assessment, indicators of suspicious transactions and activity, practical examples and guidance on simplified and enhanced CDD measures, indicators of beneficial ownership concealment, an explanation of the key functions, skills and knowledge of the AML/CFT officer in charge, an explanation of self-assessment by the obliged entities. Since this guidance is adopted relatively recently, it is not possible to assess its effectiveness at the time of the on-site mission.

1056. In view of the recent launch of VASPs and DNFBPs, the AFSA objectively believes that additional awareness-raising of obliged entities specialists is required, and provides training not only to the obliged

entities, but also to the staff of AFSA. From January 2021 to September 2022 25 trainings on various AML/CFT topics were conducted for the staff of the AFSA. According to the assessment team, this has a positive impact on the implementation of international standards in AIFC.

1057. The MDD has prepared regulations and guidance documents that form the basis for understanding what VASPs not registered in the AIFC must do in the AML/CFT sphere. There were no VASPs not registered in the AIFC at the time of the on-site mission.

Overall conclusion on IO.3

Financial institutions

1058. Supervisory authorities regulate, control and monitor FIs' compliance with the AML/CFT legislation, as well as controls to prevent criminals from owning shares in FIs through licensing or registration of their activities, and through subsequent regular inspections, taking into account certain risk indicators of FIs' activities.

1059. At the same time, supervisors understand risks as the involvement of FIs in the commission of predicate offenses, and accordingly, the quantitative and qualitative criteria for the FIs risk assessment used to conduct risk-based supervision are not based on ML/TF risks per se. Supervisors have not identified instances of the involvement of FIs in ML/TF schemes.

1060. Supervisors apply various tools of a risk-based approach in AML/CFT supervision, but the ARDFM does not fully implement consolidated supervision of the international financial groups.

1061. The application of sanctions and supervisory response measures are effective in most cases in eliminating identified breaches and preventing their repeating in the same FIs, but have no effect in reducing the number of breaches of AML/CFT legal requirements in general.

DNFBPs and VASPs

1062. All DNFBPs in the country are registered and/or licensed and/or notified the supervisory authority when they commenced operations. Supervisors are generally aware and understand the risks in the sectors they supervise, and take mitigation measures. However, the measures are mainly focused on prevention and are not related to addressing the preconditions for the identified ML/TF risks, with the exception of certain measures taken by the MCS.

1063. Prudential supervision is carried out by the government authorities all the time. Depending on the sector, supervision may be carried out on a semi-annually, quarterly or monthly basis. The results of the NRA have influenced the ability of supervisory authorities to conduct unscheduled inspections, in addition to monitoring. The FMA, using the "Personal Account" online service on the FMA portal, checks the performance of the obliged entities on a daily basis and is able to respond promptly to AML/CFT deficiencies in their performance. The government authorities supervising DNFBPs have not shown much activity in using this service to detect/prevent AML/CFT breaches.

1064. The forms of corrective measures and penalties in relation to obliged entities are not varied, the AML/CFT violations detected do not tend to decrease, consequently are not deterrent and, therefore, not fully effective. Measures of administrative liability are only imposed by courts. There is no possibility to hold obliged entities officials, who are not quasi-state entities, administratively liable. At the same time, the work of supervisory authorities and SRBs is aimed at prevention.

1065. Although the FMA does a great deal of work to clearly understand the AML/CFT obligations of the obliged entities, other supervisors are less active in this direction and rely more on the FMA and industry SRBs.

1066. The AFSA uses a risk-based supervisory approach model developed on the basis of the classic risk management approach (inherent risks minus controls constitute residual risk), taking into account the inherent business characteristics of AIFC members based on the available individual risks of the obliged entities. Quantitative and qualitative criteria are taken into account in this model. At the time of the on-site

mission, there were no inspections completed up to the date of identification and sanctioning of AIFC members.

1067. The Republic of Kazakhstan has prepared the legal framework for the operation of the VASPs. At the time of the on-site mission, there were no VASPs outside the AIFC.

1068. **Kazakhstan is rated as having moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Action

Key Findings

1. Information on the types of legal persons and the specifics and procedures for their establishment is public and available.

2. The competent and other authorities of Kazakhstan have generally demonstrated certain understanding of the vulnerabilities of legal persons, limited to examples of criminal prosecutions for predicate offences without in-depth analysis and involvement of all relevant authorities and the private sector.

3. The risk of illegal use of legal persons for criminal purposes is high. No cases of misuse of legal persons for TF purposes were identified at the time of the on-site mission.

4. Although the Civil Code defines bearer securities as a form of issue of securities, the legislation on the securities market, on joint-stock companies, investment and venture funds does not stipulate the issuance of bearer securities. There are no bearer securities in turnover.

5. In order to mitigate the risks of misuse of legal persons, a number of tools have been developed and implemented in the country. These include risk-based controls carried out by the SRC, but related only to tax administration and the prevention of the involvement of legal persons in predicate offences.

6. The State Database "Legal Persons" (SDLP) contains basic information on legal entities and information on beneficial owners of legal entities – residents of the Republic of Kazakhstan. The SDLP is public, however, the information related to BOs is only available to law enforcement and special and supervisory authorities, FMA and STBs. The source of BOs data is the information provided by applicants during the registration of legal entities. Provided BO information is not verified by the registration authority for accuracy and relevance.

7. FMA maintains its own register of BOs of legal entities, which unites data from several sources, such as the SDLP, AIFC register, securities depository, as well as the results of tactical analysis and materials of interaction with law enforcement agencies on relevant investigations. The FMA's register is available to law enforcement and special agencies and can also be used to initiate data changes in the SDLP.

8. Non-resident legal entities' BOs are identified by the FI or DNFBP at the time of accepting services by collecting and examining data from available public or commercial databases. Data on BOs of non-resident AIFC members are identified and verified quite effectively. The relevant information is provided to the competent authorities upon request.

9. The law does not stipulate activities of legal arrangements on the territory of the Republic of Kazakhstan. However, the AIFC developed regulatory documents on trusts. At the time of the on-site visit, no trusts were registered with the AIFC. The AIFC has developed no legal basis for activities of other types of legal arrangements.

10. Several types of sanctions are applied to legal entities, including corrective measures, administrative fines, blocking of bank deposit accounts, collection requests for tax arrears, imposition of fines and penalties. Penalties for failure to provide information are generally not applied.

Recommended Action

1. The authorities of the Republic of Kazakhstan should systematically improve competent authorities' understanding of ML/TF risks posed by legal persons involving more sources of

information, as well as taking into account links between legal persons and their specific activities, geographic exposure to risk.

2. The registrators should take measures to arrange verification of information of BO of a legal person, submitted during registration, as well as to determine liability of applicants for providing unreliable information during registration (re-registration) of a legal person.

3. It is recommended to establish a regular exchange of information on BO accumulated by FMA, law enforcement agencies and the private sector when dealing with legal entities, with the registering authority to update the information on BOs in the SDLP.

4. The practice of applying proportionate and dissuasive sanctions should be introduced for legal entities and legal arrangements that do not provide registration authority with the changes in basic and BO information or provide it not in a timely manner.

1069. Immediate Outcome considered and assessed in this section is IO.5. Recommendations 24-25 and elements of R.1, 10, 37 and 40 are used for evaluating effectiveness.

7.2. Immediate Outcome 5 (Legal Persons and Arrangements)

7.2.1. Public Availability of Information on the Creation and Types of Legal Persons and Arrangements

1070. Information about the types of legal persons, special features and procedures for their creation is publicly available, the relevant detailed information is posted on the website of the State Corporation "Government for Citizens"[31], and similar data about the AIFC member companies – on the AIFC website[32].

1071. The law does not stipulate activities of legal arrangements on the territory of the Republic of Kazakhstan. The AIFC developed regulatory documents on trusts (for more details, see the analysis on Rec. 25). However, at the time of the on-site visit, no trusts were registered with the AIFC. The AIFC has developed no legal basis for activities of other types of legal arrangements. No foreign legal arrangements have been identified in the country.

Registration of Legal Persons

1072. All legal persons created in the Republic of Kazakhstan are subject to state registration (see Table D in cl.199). The registration procedure stipulates checking the compliance of the submitted documents with the law, issuing a registration certificate with the assignment of a business identification number, as well as entering the relevant information into the National Register of Business Identification Numbers – State Database "Legal Persons" (SDLP). The website of the State Corporation "Government for Citizens" lists the services and indicates their name, documents required for submitting an application, time frames and cost of the services, as well as regulations governing the state registration procedure[33].

1073. Registration of legal persons is declarative (for medium-sized and large business entities) and notification-based (for small-sized business entities and individual entrepreneurs). It is carried out by contacting the registration authority with submission of documents in paper form or mainly online (subsection "Registration and Business Development" on the website of the registering authority)[34]. To do this, the applicant must log in and obtain an EDS (electronic digital signature)[35]. If there are founders, each founder must sign the application with an EDS. The application is processed within 2 business days.

1074. First of all, the registration authority checks whether there are grounds for denial of registration, the list of the grounds is determined by the law[36]. For this, integration interaction with the state databases "Legal Persons" and "Natural Persons" is ensured. The founders (managers) are automatically checked to

31 https://egov.kz/cms/ru/
32 https://aifc.kz/ru/
33 https://gov4c.kz/ru/services/pasporta-gosudarstvennykh-uslug/77/
34 https://egov.kz/cms/ru/categories/state_support_measures/
35 https://egov.kz/cms/ru/services/business_registration/pass042com_mu/
36 Art. 11 of RK Law on State Registration of Legal Persons and Record Registration of Branches and Representative Offices.

find out if they are legally incapable (have limited legal capacity), deceased, missing, declared dead, presence or absence on the lists of FT/PF, or whether they submitted invalid identity documents. If the above is true, a legal person will not be registered.

Table 5.1. Information on the number of denials of state registration of legal persons

Grounds for denial	2018	2019	2020	2021
Violation of the procedure for creation, re-registration and reorganization of a legal person established by the legislative acts of the Republic of Kazakhstan, non-compliance of the constituent documents with the law of the Republic of Kazakhstan	0	100	317	1200
Failure to submit a certificate of ownership and merger or a separation balance sheet or the absence of provisions on legal succession during reorganization of the legal person in these documents	0	2	6	0
If the individual being a founder (participant, member) and (or) head of a legal person is the sole founder (participant, member) and (or) head of non-operating legal persons	0	245	494	689
If the individual being a founder (participant, member) and (or) head of a legal person is included in the list of entities and persons involved in the financing of proliferation of weapons of mass destruction, and (or) in the list of entities and persons involved in the financing of terrorism and extremism, in accordance with the legislation of the Republic of Kazakhstan, with the exception of shares (stakes in the authorized capital) confiscated and (or) recovered subject to a court decision	0	0	1	0
If the individual being a founder (participant, member) and (or) head of a legal person is declared legally incapable or having limited legal capacity	0	0	2	0
If the individual being a founder (participant, member) and (or) head of a legal person is declared missing, deceased, registered as deceased, or his status is not defined	0	4	7	0
If the individual being a founder (participant, member) and (or) head of a legal person has an outstanding or unspent conviction for crimes under Articles 237, 238 of the Criminal Code of the Republic of Kazakhstan	0	423	940	456
If during state registration the founder (individual and (or) legal person), its founders, the head of the legal person, the founder and (or) the head of the legal person being the founder (participant, member) of the legal person are debtors in enforcement proceedings, except for debtors in enforcement proceedings to collect recurring payments with no debt in enforcement proceedings to collect recurring payments during more than three months	0	803	1574	2547
If during state registration new founders (participants, members) and (or) persons alienating a share are debtors in enforcement proceedings, except for debtors in enforcement proceedings to collect recurring payments with no debt in enforcement proceedings to collect recurring payments during more than three months	0	589	904	1256
Submission of lost and (or) invalid identity documents	0	102	221	268
Judicial acts and resolutions (bans, arrests) of bailiffs and law enforcement agencies	0	107	141	589
Unless otherwise provided by the laws of the Republic of Kazakhstan or a judicial act, registration actions are suspended until the elimination of the circumstances that are grounds for the suspension, but not more than for one month. If the circumstances that are grounds for the suspension are not eliminated within one month, registration is denied, with the exception of obtaining an expert opinion.	0	80	114	132

1075. If there are no grounds for denial of registration of a legal person, the state revenue authorities check the individuals and legal persons mentioned in the application using the “Know Your Client” procedures

(scanning of identity documents, analysis of open source information), as well as through the commercial databases (lists with information about involvement in money laundering, terrorist financing, participation in court cases on financial crimes, status of PEPs and their close relatives, sanctions/embargoes). It should be noted that the results of this inspection do not constitute grounds for refusing to register a legal entity.

Table 5.2. Structure of registered legal entities by legal form (percentage)

	2018	2019	2020	2021
Limited Liability Partnership	42,5	55,03	61,66	67,15
Partnership with Additional Liability	0,22	0,21	0,19	0,13
Production Cooperative	6,34	4,99	4,25	3,81
General Partnership	0,73	0,56	0,47	0,25
Limited (Commandite) Partnership	0,05	0,04	0,03	0
Joint-Stock Company	1,20	0,92	0,76	0,58
Branch	39,82	30,71	25,97	24,82
Representative Office	9,13	7,55	6,67	5,34

Table 5.3. Number of registered commercial entities

	2018	2019	2020	2021
Limited Liability Partnership	36,687	33,974	31,769	36147
Partnership with Additional Liability	65	65	55	51
Production Cooperative	472	311	428	438
General Partnership	19	21	15	13
Limited (Commandite) Partnership	3	6	2	1
Joint-Stock Company	39	28	21	13
Branch	975	1147	929	1254
Representative Office	181	189	151	195

Table 5.4. Information about business entities with foreign ownership

	2018	2019	2020	2021
Total	31,467	32,740	34,416	37,851
of them:				
Russia	9,987	10,513	10,915	11,506
Turkey	3,439	3,396	4,082	4,203
China	2,447	2,592	2,672	2,787
Kyrgyzstan	1,236	1,427	1,909	2,037
Uzbekistan	1,773	1,838	1,896	1,928
Ukraine	1,133	982	1,013	1,142
Azerbaijan	794	848	890	940
Germany	874	841	870	923
Republic of Korea	833	800	794	815
Netherlands	848	638	730	778
USA	732	662	709	769
United Kingdom	664	583	608	628
India	474	491	490	511

1076. The AIFC members are registered by the Registrar of Companies of AFSA (further in this section – the AIFC Registrar) based on an online application submitted via the self-service portal[37] or by contacting the office of the Registrar of Companies of AFSA directly (see Table E in para 201). The application is accompanied by constituent and other documents that are checked, in particular, through the implementation of KYC and Customer Due Diligence procedures in relation to the chief executive officer (CEO), shareholders and beneficiaries.

1077. After successful registration, the AIFC member company gets a certificate with the assigned business identification number and individual QR code. The relevant information is entered into the National

[37] http://www.digitalresident.kz/

Register of Business Identification Numbers, reflected in the AIFC Public Register, sent to the Ministry of Justice and entered into the SRC database.

1078. If the registration data of the AIFC member company change, the AIFC Registrar shall be notified within 14 days on paper or through a special online portal[38]. The AIFC Registrar implements the check via commercial databases in relation to all persons, including the director, CEO, shareholders and beneficiaries.

Availability of Basic Information About Legal Person and the Beneficial Owner

1079. All legal persons, branches and representative offices are assigned unique business identification numbers (further in this section – BIN) which are included in SDLP[39]. Being under the jurisdiction of the Ministry of Justice and integrated with 34 information systems of state authorities, the SDLP contains information about the name of the legal person, its place of registration, BIN, participation shares, head, individual identification number (further in this section – IIN), type of economic activity, form of incorporation, submitted by the applicant when registering information on the beneficial owner, etc., i.e. basic information about all legal persons registered in the country. The SDLP is a unified source of data on legal persons, that maintain interdepartmental electronic communication in the provision of public services and is used as necessary by the competent authorities. The SDLP is integrated with almost all interested state authorities which receive information automatically upon request.

1080. Publicly available information about a business entity includes the surname, name, patronymic, name of an individual entrepreneur, name and date of registration of a legal person, IIN, legal address (location), type of activity and other information that can be obtained without restrictions upon request at the website of the registration authority[40]. The relevant electronic services for searching taxpayers are publicly available on the SRC Internet portal.[41]. Taxpayer information that does not constitute a tax secret and is posted on the SRC Internet portal is updated by integrating information systems on a daily basis. These services are also implemented in the mobile app "E-salyq Azamat".

1081. Information on the creation, types and characteristics of legal persons registered in AIFC is publicly available and posted on the website of the AFSA[42]. It includes data on BOs, shareholders, partners, founders, directors, BIN, address, country of registration, number and type of license, status, date of registration and permitted type of activity, full name of the director, full name or name of the shareholder, size of authorized capital (for private companies, public companies and special purpose companies). The amended data of the AIFC members are sent to the MoJ for entry into the SDLP.

1082. In addition to basic information on legal entities, the SDLP contains information on their BOs. The BO information is restricted and available to the competent state authorities and STBs.

1083. During the registration of a legal person the applicant provides the BO information which is entered into the SDLP, and the registrar does not check it for accuracy and relevance. However, an analysis of the SDLP revealed cases where the information on the founders and BOs do not coincide, and this fact to a certain extent demonstrates the effectiveness of the survey of applicants who are aware of the responsibility for providing deliberately false data on the BOs.

Table 5.5. Information on discrepancies between the information on the founders and BOs in the SDLP

Year	Number of legal persons where the information on BO matches the information on the founders	Number of legal entities where the information on BO does not match information on the founders
2019	17,177	1,143
2020	29,058	4,840
2021	21,702	2,510
2022	30,319	5,153
Total	98,256	13,646

[38] https://digitalresident.kz/
[39] http://data.egov.kz/datasets/view?index=gbd_ul/
[40] https://data.egov.kz/datasets/view?index=gbd_ul/
[41] https://kgd.gov.kz/ru/services/taxpayer_search/entrepreneur/
[42] www.afsa.aifc.kz/

7.2.2. Identification, Assessment and Understanding of ML/TF Risks and Vulnerabilities of Legal Persons

1084. During the on-site visit, the competent authorities of the Republic of Kazakhstan demonstrated a certain understanding of how legal persons can be misused for criminal purposes. Legal persons are misused for cash-out, tax evasion, as shell companies, etc. At the time of the on-site visit there were no cases of misusing legal persons for TF purposes.

1085. The assessment of vulnerabilities of legal persons was carried out as part of the ML/TF NRA. In addition, the country has prepared a separate report on vulnerabilities of legal persons and legal arrangements to ML/TF schemes (further in this chapter – the Report on vulnerabilities). It includes detailed information on the relevant sector as of January 1, 2021, an overview of the mechanisms for recording and storing basic and extended information on legal persons, as well as existing vulnerabilities and risks of their misuse for committing predicate offences.

1086. During the assessment, a large amount of data has been used, and in addition to studying the laws, practical features of legal persons' activities, their quantitative indicators have been considered. In particular, materials of criminal cases involving legal persons have been used. Also, STRs that dealt with legal persons' transactions have been examined. For example, during 2018-2020, more than 1 million STRs involving legal persons of various forms of incorporation were sent to the FMA by the obliged entities. For example, 499 reports sent in 2018-2020 were used by FIU for developing 45 schemes of allegedly criminal groups by analytical methods. Typologies for gaining and (or) legalizing criminal proceeds using limited liability partnerships and business entities of other forms of incorporation are systematically developed and posted on the official FMA website.

Table 5.6. Number of suspicious transaction reports involving legal persons

Form of incorporation	Number of STRs for 2018-2022
Limited Liability Partnership	623,140
Partnership with Additional Liability	324
Production Cooperative	3,601
General Partnership	101
Limited (Commandite) Partnership	206
Joint-Stock Company	83,137
Individual Entrepreneurs	606
Institution	15,787
Public Association	38,707
Foundations	26,608
Consumer Cooperative	19,174
Religious Associations	1,407

1087. According to the conclusions made by the country, the most common forms of incorporation in the Republic of Kazakhstan are mainly LLP and Individual Entrepreneur, which is explained by minimal requirements for the authorized capital (their absence for Individual Entrepreneurs), ease of registration, and the existence of special tax regimes. Competent authorities and the private sector confirmed the NRA findings and noted that most of the legal persons registered in the territory of the Republic of Kazakhstan have been created in the form of LLC, which are most commonly used for criminal purposes. In general, the assessors agree with the country's findings that the main ML/TF risks are associated with legal persons in the form of LLPs. At the same time, the above arguments cannot be considered as a comprehensive and in-depth analysis of the risks of LLPs, since they are standard (almost inherent) characteristics of this type of legal persons. In this regard, the Kazakh authorities could have increased their understanding of the risks in the country by further strengthening the links of legal persons with the specific activities they carry out, the supply chains used by Kazakh legal persons, and the geographic exposure to risk.

1088. According to the Report on vulnerabilities, one of the practical problems is communication of legal persons with shell companies (unreliable entities) in order to evade paying taxes to the budget, and this is caused by "inoperative provisions of the Criminal Code" of Art. 216 (Issuing Invoice without Performing

Work, Shipping Goods) and Art. 245 (Tax Evasion by an Entrepreneur) of the Criminal Code of the Republic of Kazakhstan. At the same time, the ML/TF NRA mentioned that, after the *fact of issuing fictitious invoices*, the detection of crimes increased by half (from 269 in 2019 to 417 in 2020), *the closure of criminal cases almost doubled from 30 to 57% (in 2020 – 393 of 693 cases, in 2019 – 118 of 396 cases).*

1089. The law enforcement authorities mentioned that in practice the following frequently encountered typologies of misuse of legal persons for criminal purposes were revealed: a) using legal persons for illegal cash-out of funds; b) using economic entities registered by foreign citizens in illegal activities; c) using microfinance organizations for committing crimes, primarily for the purpose of building financial pyramids, the main purpose of which is obtaining material benefits through financial fraud; d) evasion of taxes or other obligatory payments, primarily by issuing fictitious invoices; e) using online casinos in illegal activities.

Case Study 5.1

In 2020, members of a criminal group were caught red-handed in the Karaganda region when cashing out 6.3 million KZT through an ATM. During 3 years, this group has withdrawn 4 billion KZT through ATMs. During the search, 6.4 million KZT, 5.5 thousand euros, bank cards of several banks of Kazakhstan were seized, as well as accounting documents and seals in the amount of 25 pieces.

Case Study 5.2

In 2020, the courts of the Aktobe region canceled state registration of LLP "E" and LLP "A", the head and founder of which was G, a non-resident citizen of the Republic of Kazakhstan. The firms have been misused for criminal purposes, and the reason for canceling their registration was the lack of an entry visa of a foreigner as a business immigrant. This foreign citizen has opened accounts in the Almaty branches of major banks of Kazakhstan, which have had no suspicions when entering into business relationship.

Case Study 5.3

The SD is processing a criminal case against Mr. D., who, in a group with other persons, in the period 2019-2020 made an illegal refund of corporate income tax in the amount of 1.1 billion KZT by reflecting mutual settlements with a fraudulent enterprise in tax reports, thereby committing a crime under Art. 190, Part 4, Paragraph 2 of the Criminal Code of the Republic of Kazakhstan (Theft by Fraud).

During a parallel financial investigation, the suspects' property totaling to 2.3 billion KZT was detected and seized.

As a result of the analysis of the financial component of the above fraudulent enterprise, a legal person was detected which had issued fake invoices to one of the large city-forming enterprises in the amount of 486 million KZT. Pre-trial investigation into this fact was initiated under Art. 216, Part 3, paragraph 2 of the Criminal Code of the Republic of Kazakhstan *(Issuing Invoices without Performing Work, Rendering Services, Shipping Goods).*

Case Study 5.4.

In 2020, almost 17,000 citizens bore damages from the activities of certain financial organizations (G LLP, E LLP, V LLP), in the amount exceeding 21 billion KZT. In this regard, 32 criminal cases were initiated in 14 regions of the country.

1090. Also, the country mentioned widespread activities of online casinos despite their legal prohibition, which is explained by the fact that the owners of online casinos obtain licenses in foreign countries and

carry out activities in the territory of the Republic of Kazakhstan through websites. At the same time, ineffectiveness of restricting access to the relevant websites was stated due to their possible prompt new registration, as well as the use of special software and hardware by citizens of the country.

Case Study 5.5

In 2018-2020, based on the results of Internet resources monitoring, the EIS identified 143 websites providing online casino services (2018 – 59, 2019 – 67, 2020 – 47), which were blocked by the Telecommunications Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

1091. As part of the ML/TF NRA, the role of individual entrepreneurs and private companies registered as AIFC member companies was studied in terms of ML vulnerability. However, no relevant conclusions were made. At the same time, the Kazakh authorities have insufficient understanding of vulnerabilities and risks posed by misusing service providers, for example, intermediaries providing corporate, accounting, legal services to legal persons, despite the fact that, according to open Internet sources, activities of such organizations are widespread in the Republic of Kazakhstan[43].

1092. The ML/TF NRA also assessed such category of legal persons as NPOs operating in the Republic of Kazakhstan. Besides main activities, the NRA provides information on the sources of funding for NPOs (for example, *admission and membership fees; one-time and regular payments from founders, participants (members); voluntary asset contributions and donations, etc*.). According to the assessors, the competent authorities of the Republic of Kazakhstan are closely monitoring activities of NPOs, especially their funding channels. At the same time, the facts of failure to submit reports is stated as a factor that increases the risk of the NPO sector in terms of possible use of activities of such organizations for terrorist financing. See IO.10-related section of the MER for more details on the assessment of NPOs.

1093. The competent authorities demonstrated, in general, good understanding of vulnerabilities of legal persons and the way they can be misused for criminal purposes. The supervisors demonstrated similar understanding and confirmed the NRA results in terms of vulnerabilities inherent in legal persons. Along with that, the typologies of misuse of legal persons for ML and predicate offences described in the Report on vulnerabilities do not seem to be fully developed, since they are based on individual examples of criminal prosecution without deep analysis and involvement of all interested authorities and the private sector. In this regard, the assessors conclude that the justification described in the Report on vulnerabilities for findings on the exposure of legal persons to ML and FT risks is not complete.

1094. It should also be mentioned that general features of the approach to risk assessment affected the assessment of legal persons' vulnerabilities and risks, which was more focused on legal persons' involvement in predicate offences.

1095. The AIFC has implemented risk assessment measures during the registration period of members, which are regularly updated, as necessary. A Practical Guidance to the AIFC Rules on Combating the Legalization (Laundering) of Criminal Proceeds and the Financing of Terrorism has been prepared and is being implemented. Separate detailed sections of the Practical Guidance cover the analyzed issues. According to the Report on vulnerabilities, no facts of involvement of legal persons – AIFC members in ML/TF schemes were identified during the analyzed period. The risk of involvement of legal persons – AIFC members in ML schemes is medium, in TF – medium.

7.2.3. Measures to Mitigate Risks Related to Misuse of Legal Persons and Arrangements

1096. Certain dissuasive measures are taken in the Republic of Kazakhstan that have an impact on preventing the misuse of legal persons. These include risk-based controls implemented by the SRC. Only the risks associated with tax administration and the involvement of legal persons in predicate offences are taken into account. In addition, the SRC monitors legal persons that do not conduct financial and economic

[43] https://axisa.uchet.kz/

activities. The tax authorities conduct regular on-site inspections to verify compliance of the main registration data, in particular, actual location of the management bodies at the place of registration.

1097. If violations are revealed, the tax authorities issue an order to eliminate them, and if violations are not eliminated within 10 days, the bank account of the legal person is blocked. If there is no subsequent response, the SRC checks the counterparties of the legal person and gathers materials to be handed over to the law enforcement agencies.

1098. Within its competence, the SRC initiates in the court the invalidation of the registration of such legal persons (see para 1118). In addition, the SRC is empowered to block the access of untrustworthy legal persons to the electronic invoicing system, which prevents them from issuing invoices. Based on information from the EIS of FMA, the SRC blocked the issuance of invoices to 2 thousand legal persons with the characteristics of "one-day" companies during the analysed period.

1099. Information on the involvement of legal and natural persons in illegal activities based on the materials of operative checks, criminal cases and analytical work is transmitted by the criminal prosecution authorities to the FMA. In order to inform the obliged entities, the list of such persons is posted on the FMA website. Based on the information provided to the EIS of FMA, the STBs have refused to establish business relations with 4,6 thousand and terminated business relations with 2,1 thousand customers.

1100. If high risks are identified among the AIFC member companies, the AFSA organizes inspections, resulting in demands to eliminate the identified deficiencies.

7.2.4. Timely Access of Adequate, Accurate and Up-to-Date Basic Information and Beneficial Ownership Information in Relation to Legal Persons

1101. The Kazakh authorities have taken a number of measures to improve the accuracy and reliability of the information contained in the State Database “Legal Persons”. These measures are aimed at preventing the misuse of legal persons through nominees (front men), non-operating (shell) companies.

1102. At the same time, BO information provided by the applicants is entered into the relevant database during registration of legal persons. During the on-site visit, the assessors were given an explanation that the applicant is responsible for reliability of these data, which is confirmed by his signature or a mark in the appropriate check-box that proves that legal responsibility is assumed by him. However, no clear definition of such responsibility has been identified. At the same time, it confirmed the findings of the Report on vulnerabilities, according to which the registration authorities do not verify the BO information included in the SDLP.

1103. According to the information provided by the MOJ, the Registrar verifies the data on the resident founders, BOs and managers by comparing the data with the State Database “Natural Persons” in real time. Data on the founders - legal persons is similarly compared with the SDLP.

1104. According to the findings of the Report on vulnerabilities, there are difficulties in the country related to identifying the BO of a legal person when the founder is an individual or legal person that is a non-resident of Kazakhstan.

1105. Subsequently, the entered data on BOs can only be corrected at the request of the legal person itself and its representatives. The Registrar cannot make changes to the basic and extended information about legal persons maintained in the SDLP. If the tax authorities become aware of inaccurate (unreliable) information regarding the legal person included in the database, they have the right to file a lawsuit in court to invalidate registration. Besides, data may be updated with the initiative of FMA (see para 1110).

1106. The country’s Report recognizes that deficiencies in terms of promptness and relevance of obtaining BO information increase vulnerability of legal persons of the Republic of Kazakhstan to a high level, vulnerability of the AIFC – to a medium level.

1107. It should be mentioned that the above deficiencies are compensated by good understanding of the essence of BO demonstrated by the EIS of FMA, as well as their ability to quickly identify the BOs of legal

persons.

Case study 5.6

The EIS of FMA analysed the suppliers of the entity “N” controlled by citizen Sh. And identified companies in which citizen S., Sh.’s former spouse, was a founder, for example LLP “D”. In this company, a certain citizen N., who was also a founder of LLP “T”, became a founder after S. Thus, the beneficial owner of LLP “D” and LLP “T” was 188pprox.188in to be Sh.

Case study 5.7.

In an analysis of companies, citizen K. was found to have received pension contributions between 2007 and 2020 in companies controlled by citizen B. during the same period that B. moved from company to company (LLP “K”, LLP “R”, LLP “N”, LLP “A”). At the same time, in LLP A, Citizen K. was the manager and Citizen B. was the founder.

In addition, K. received pension contributions from the representative offices of companies G (UAE) and N (UAE) in Kazakhstan, the head of which was Citizen S., who also worked in companies controlled by Citizen B..

Thus, it was established that Citizen B. was the COO of the network of interconnected companies due to his ability to influence the aforementioned companies through persons close to him.

1108. Until February 2022, the tactical units of the FMA conducted the identification of the BO by analysing the STRs of obliged entities. Since February 2022 this work has been methodologically streamlined and systematised in the form of a regularly updated automated module "Register of beneficial owners and persons likely controlling a legal person" (hereinafter referred to as the "FMA Register").

1109. The FMA Register contains information on all legal persons in the country, collected from sources of data both on officially registered BOs (SDLP, AIFC, securities depository) and on alleged ultimate BOs (analysis of STRs of obliged entities, law enforcement information, data of foreign FIUs, internet intelligence, etc.). The FMA Register has a permanent updating of information on the BOs based on the feedback of the Register's users.

1110. Information from the FMA Register is available to competent authorities upon request. For example, in 2022, the FMA received 321 requests from LEA, which used the BO information from the Register.

1111. In case of discrepancies between the data in the Register and the SDLP, the FMA sends a notification to respective justice department with a request to arrange amendment of SDLP data by the legal person. In this way, the SDLP data is updated and kept up to date in terms of data on the legal persons coming over the attention of the FMA.

Case study 5.8

During the pre-trial investigation into the evasion of taxes and other obligatory payments to the budget in relation to LLP "O" in March 2022, the Shymkent EID investigated the counterparties of LLP "O", including LLP "R". As a result of the study, discrepancies were revealed in the data on the BO of LLP "R" indicated in the SDLP and the actual BO of LLP "R"

Based on the results of this fact, the EID of Shymkent sent an official request to the Department of Justice of Shymkent with a request to check and consider bringing LLP "R" to administrative responsibility.

1112. The AIFC Registrar collects, cross-checks and maintains basic and BO information related to all residents of AIFC. The AIFC residents are required to maintain and annually submit annual reports, including registers of shareholders, directors and BOs, within 6 months after the end of the reporting year.

1113. At the time of the on-site mission, 1,543 AIFC members were registered in AIFC. There are a total

of 1,670 individuals who are active BOs of AIFC members in the register.

7.2.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

1114. At the time of the on-site visit, no legal arrangements, including foreign ones, were registered on the territory of the Republic of Kazakhstan. Also, illegal activities of such legal arrangements were not revealed.

1115. Despite the existence of a legal basis for activities of legal arrangements in the form of trusts, the latter have not been created and have not operated on the AIFC territory. No other types of legal arrangements are envisaged in AIFC.

7.2.6. Effectiveness, Proportionality and Dissuasiveness of Sanctions

1116. Legal persons must submit information on amendments in their charter documents, regulations on their branches (representative offices), as well as on changes in other data, including those concerning: the managers; transfer of the share capital in trust management; increase in the charter capital; main type of economic activity within 1 month of such changes, on a declaratory basis. There is administrative liability for failure to comply with this requirement.

Table 5.7. Information on detected failures to amend registration information

Period	2018	2019	2020	2021
Number of detected violations	545	306	117	110
repeatedly of them	0	0	0	0

1117. The tax authorities actively implement several types of sanctions against legal persons, in particular, corrective sanctions, administrative fines, and they also have the right to block a bank current account, make collection orders for payment of tax debts, impose fines and charge penalties for tax violations.

1118. Along with the sanctions, the tax authorities may file lawsuits to invalidate registration or re-registration of legal persons. It should be mentioned that according to the information received from the tax authorities during the on-site visit, the reason for implementing this measure is mainly the absence of management bodies of the legal person at the place of registration.

1119. In 2018-2022 6,201 applications were submitted to the judicial authorities (2018 - 901; 2019 - 959; 2020 – 844, 2021 – 1 932, 2022 - 1 565), on which suit claims for invalidation of registration (re-registration) were satisfied.

Table 5.8. Information on the number of re-registered legal persons

Year	The number of re-registered legal persons
2018	41 254
2019	48 597
2020	54 215
2021	61 154
2022	71 541
Total	**276 761**

Table 5.9. Number of liquidated legal persons

	2018	2019	2020	2021
Production Cooperative	464	380	331	412
Consumer Cooperative	1	-	-	5
Partnership with Additional Liability	14	23	18	25
State Enterprise	84	141	56	58
Limited Liability Partnership	12,641	20,134	15,947	23 458
Limited (Commandite) Partnership	5	3	2	1
General Partnership	130	39	45	54
Joint-Stock Company	65	84	70	61

1120. Lists of taxpayers with invalidated registration (re-registration) are posted on the official website of state revenue authorities[44].

Overall Conclusions on IO.5

1121. Information about the types of legal persons, special features and procedures for their creation is publicly available. There is a state register (SDLP) containing basic and BO information of the legal persons. The BO information provided by the applicants during the registration of legal persons is not checked by the registering authority for accuracy and relevance. However, there are alternative ways to verify the BO information, including through the FMA Register, which is updated based on the results of tactical analysis and interaction with the law enforcement and special authorities.

1122. The data of the SDLP in terms of BO information are available to the competent authorities and STBs. Information from the FMA Register is available to law enforcement and special agencies upon request.

1123. The risk of misuse of legal persons for ML is high. The country has conducted a risk assessment of legal persons, but the rationale for the conclusions about the exposure of legal persons to ML and TF risks is not fully complete.

1124. A number of mechanisms have been developed and implemented in the Republic of Kazakhstan to reduce the risks of misusing legal persons. They include risk-based control exercised by the SRC, which is related to tax administration and prevention of the involvement of legal persons in predicate offences. However, sanctions are generally not applied for failure to report changes in basic (except for location) or BO information.

1125. The law does not stipulate activities of legal arrangements on the territory of the Republic of Kazakhstan. At the same time, the AIFC developed regulatory documents on trusts. At the time of the on-site visit, no trusts were registered with the AIFC. The AIFC has developed no legal basis for activities of other types of legal arrangements. No foreign legal arrangements have been identified in the country.

1126. **The Republic of Kazakhstan is rated as having a moderate level of effectiveness of IO.5.**

[44] https://kgd.gov.kz/ru/services/taxpayer_search_unreliable/list/

CHAPTER 8. CHAPTER 8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

1. International cooperation, including mutual legal assistance, is generally carried out in a constructive and timely manner. The GPO, as a central body (along with the SC) coordinates this activity, ensures recording of requests and their timely execution. Secure electronic communication channels are used for their transmission. The FATF Global Network survey characterizes the quality of MLA's delivery in a positive way. However, feedback on the usefulness of the information provided within the framework of MLA execution is not requested on a systematic basis.

2. In the vast majority of cases, all competent authorities resort to MLA mechanisms when there is evidence of the transnational nature of the offence. Statistical information shows that competent authorities are confident in resorting to MLA mechanisms and that, in general, the assistance requested corresponds to the country's risk profile.

3. LEAs/SSAs have been successful in identifying, seizing and confiscating assets abroad, which has been facilitated, among other things, by the implementation of the Stolen Asset Recovery project in the Republic of Kazakhstan since 2016. Alternative formats of international cooperation are used, including CARIN, ARIN AP, ARIN-WCA, INTERPOL FOCAL POINT and others.

4. The authorities of the Republic of Kazakhstan generally cooperate effectively in the field of extradition and most of the relevant incoming requests are granted. In cases where a person has absconded from law enforcement authorities, the country's authorities take measures to locate and extradite him or her, or the country makes efforts to bring such persons to justice, including through letters rogatory and other appropriate mechanisms.

5. Law enforcement agencies effectively cooperate and exchange information in other forms at various international venues. Such cooperation leads to concrete practical results.

6. International information exchange through the FIU is implemented on a systematic basis, together with a wide range of counterparties and its nature is consistent with national ML/TF risks. The representatives of the FIU have demonstrated a wide range of international cooperation tools, which can cover not only the needs of financial intelligence itself, but also other law enforcement agencies. At the same time, the intensity of spontaneous information to foreign partners seems insufficient, including in cases when the relevant information available to the FIU is transmitted to the competent authorities inside the country.

7. International cooperation of FI and DNFPB’s supervisors is based on international agreements and there are no regulatory obstacles to the exchange of relevant information. The level of international supervisory cooperation is consistent with the needs of regulators and the possible risks at this stage.

8. All competent authorities are able to receive and transmit beneficial ownership information through MLA and other forms of international cooperation.

Recommended Actions

1. The Republic of Kazakhstan should systematically request feedback, accumulate and analyze information about the usefulness of the information transmitted.

2. The Republic of Kazakhstan shall take steps to develop regulatory, organizational, and methodological mechanisms for execution of the requests related to criminal use of cryptocurrencies and other virtual assets (out of the AFSA’s control) for money laundering.

3. The FMA shall catalyze spontaneous exchange of information.

4. Competent authorities shall continue to extend other forms of cooperation, paying special attention to looking for new forms of exchange of information for asset tracing, and use the MLA mechanisms therefor much more often.

1127. This chapter considers and assesses the achievement of Immediate Outcome 2. Efficiency is assessed based on Recommendations 36 to 40 as well as on the elements of Recommendations 9, 15, 24, 25. And 32.

8.2. Immediate Outcome 2 (International Cooperation)

8.2.1. Provision of constructive and well-timed mutual legal assistance and provision of extradition

1128. The Republic of Kazakhstan has developed a comprehensive legal framework for the provision MLA and the implementation of extradition. The authorities make efforts to improve and refine the legal mechanisms used in this area. The competent authorities strive to ensure that the MLA provided is timely and constructive, and that extradition is carried out promptly. The conclusions are based on the analysis of existing processes, interviews with relevant authorities, the maintenance of statistics, analysis of case law, and feedback from the FATF Global Network.

Mutual Legal Assistance

1129. In the FATF Global Network International cooperation feedback, the Republic of Kazakhstan received predominantly positive feedback on the quality and timeliness of MLA. The statistics and examples provided by Kazakhstan provide strong evidence of positive experiences with MLA in most cases, despite the geographical remoteness of jurisdictions and other related factors.

1130. The country has two central agencies (GPO and SC) which can act directly in accordance with the international treaties of the Republic of Kazakhstan or with the principle of reciprocity. At the stage of legal proceedings, MLA is provided through SC, while in the process of pre-trial procedures – through GPO.

1131. Since 2019 LEAs and SSAs (NSC, MIA, ACA, EIS) within their competence established by the criminal procedure legislation, can directly send and receive MLA requests under the Minsk and Kishinev Conventions, which explains the decrease in the total number of MLA requests received through the GP since this period (Tables 2.1-2.5).

1132. The GPO is the coordinator of the provision of MLA in the country, keeps records of requests, as well as considers all requests related to the need to obtain a court decision. The RK has flexible rules of transferring MLA requests between the competent authorities through secure electronic communication channels, allowing even in cases when the request was received by the authority in error, to send it in accordance with the competence without return or refusal in execution.

1133. The GPO is aware of all incoming requests, including in those situations where requests are sent directly to law enforcement agencies, and monitors all cases of their execution, which has been confirmed not only by statistical information, but also by the materials of annual analyses in the field of supervision of compliance with international treaties.

1134. Requests received by GPO are transferred to its own territorial bodies, as well as to the the competent authorities via secure electronic communication channels (EIS, MIA, ACA and NSC), which was confirmed during the interviews both by GPO and other bodies. in a short period of time (as a rule, up to 24 hours), which indicates sufficient efficiency (speed) of organization of their consideration. In fact, all MLA's incoming requests are executed, and they are answered in a meaningful way. No cases of lost or unprocessed requests were identified during the on-site mission.

Table 2.1 Number of request received by GPO

	2017	2018	2019	2020	2021	2022 (6 mnths)	Total
Received	**591**	**384**	**488**	**185**	**188**	**137**	**1 973**

ML/TF	0	2	1	5	9	7	24
Accepted for execution	**587**	**381**	**483**	**181**	**186**	**136**	**1954**
ML/TF	0	2	1	5	9	7	24
Refused	**4**	**3**	**5**	**4**	**2**	**1**	**19**
ML/TF	0	0	0	0	0	0	0
Transferred for execution to criminal prosecution authorities							
Total accepted for execution	**587**	**381**	**483**	**181**	**186**	**136**	**1954**
Transferred to execution — **Regional prosecutors departments**	**531**	**328**	**410**	**157**	**155**	**111**	**1 692**
To — Regional offices of EIS	63	46	55	23	22	16	225
To — Regional offices of MIA	426	257	319	118	116	86	1322
To — Regional offices ACA	26	13	24	9	13	5	90
To — Regional offices NSC	16	12	12	7	4	4	55
EIS	**4**	**12**	**10**	**3**	**5**	**11**	**45**
Central department of MIA	**48**	**35**	**59**	**21**	**24**	**10**	**197**
Central department of ACA	**1**	**2**	**0**	**0**	**1**	**1**	**5**
Central department of NSC	**3**	**4**	**4**	**0**	**1**	**3**	**15**

Table 2.2 Number of MLA requests received directly by EIS

		2019	2020	2021	2022 (6 mnths.)	Total
Received		18	14	21	33	86
	Executed	18	14	21	28	81
	Refused	0	0	0	0	0
	Number on ML/TF	0	0	0	0	0

Table 2.3 Number of MLA requests received directly by MIA

		2019	2020	2021	2022 (6 mnths.)	Total
Received		174	332	458	302	1266
	Executed	174	332	458	302	1266
	Refused	0	0	0	0	0
	Number on ML/TF	0	0	0	0	0

Table 2.4 Number of MLA requests received directly by ACA

		2019	2020	2021	2022 (6 mnths.)	Total
Received		0	1	3	0	4
	Executed	0	1	3	0	4
	Refused	0	0	0	0	0
	Number on ML/TF	0	0	0	0	0

Table 2.5 Number of MLA requests received directly by NSC

		2019	2020	2021	2022 (6 mnths.)	Total
Received		68	81	84	17	250
	Executed	68	81	84	17	250
	Refused	0	0	0	0	0
	Number on ML/TF	0	0	0	0	0

1135. According to the information provided by the country, MLA requests were received for the following categories of crimes: against property (fraud, theft, embezzlement, including embezzlement of budget funds) - 30.5% of the total number of requests; in the sphere of economic activity (tax evasion, economic smuggling, etc.) - 14.5%. economic activity; corruption - 8.7 %; terrorism and extremism - 2.1 %; drug trafficking - 5.2 %; against the person (murder, rape, bodily harm, etc.) - 22.1 %; other - 16.9 %. These statistics show that the inquiries correspond to the country's risk profile for predicate crimes.

1136. The key countries sending MLA requests to the Republic of Kazakhstan are the following: Russia - 605 (30.6%), Turkey - 380 (19.2%), Belarus - 236 (11.9%), Uzbekistan - 122 (6.1%), Kyrgyzstan - 96

(4.8%), Latvia, Lithuania - 45 (2.2%), Poland - 38 (1.9%), Azerbaijan - 24 (1.2%), Czech Republic - 21 (1%), USA - 17 (1%). Thus, the list of countries sending MLA requests to the RK corresponds to the directions of financial flows (export-import) of the country.

1137. Expert consultations and meetings are periodically held with these countries, discussing issues of mutual legal assistance, problematic issues and ways to solve them, which demonstrates a constructive approach of the Republic of Kazakhstan to ensure the effectiveness of the assistance provided. For example, as a result of one of these meetings to discuss the quality of the executed request, the parties came to an agreement to create a joint investigative team (Example 2.1). This work is an indicator of the increased level of feedback from the ML partner that resulted in the identification of new ML schemes, criminal associates, and other jurisdictions involved in the commission of criminal activity. The assessment team was shown by the assessment team that similar work is being done with other jurisdictions making ML requests.

Case Study 2.1 Creation of joint task force

In the course of the GPO's discussions with the Latvian side on the quality and completeness of MLA's provision, an in-depth analysis of each request was conducted. As a result, it was found that Latvian law enforcement authorities investigated a number of criminal cases against officials of Latvian banks. The head of one of the banks, a Latvian citizen Z., assisted in the transfer of money from Kazakh banks. Having established these circumstances and the existence of criminal cases in Kazakhstan and Latvia, the parties held additional negotiations in Latvia, where an agreement was reached to create a joint task force between the law enforcement agencies of Kazakhstan and Latvia. The Prosecutor General's Offices of Kazakhstan and Latvia concluded an agreement to establish a joint interstate investigative task force.

1138. At the same time, despite the above example and the fact that representatives of competent authorities indicated the quality of execution of requests as one of their priorities, the understanding of its criteria is based mainly on their own practice and does not always take into account the experience of using the responses provided in foreign jurisdictions to which the MLA is provided. Despite the fact that competent authorities have close contacts with representatives of foreign competent authorities and can receive information on the results of the use of sent responses in a routine manner, GPO and LEAs/SSAs should more often request feedback from the competent authorities of foreign countries.

1139. During the on-site mission the GPO provided detailed information on the consideration of 24 ML requests during the evaluation period, all of which were executed in full. 13 of them came from Latvia, 3 from Poland, 2 from the Czech Republic, 2 from Moldova, 1 from Kyrgyzstan, 1 from Belarus, 1 from Ukraine and 1 from Switzerland. The MLA requests mainly concerned possible laundering of criminal proceeds in order to establish the origin and ownership of funds. Foreign competent authorities requested registration and banking information, data on tax deductions, interrogation of witnesses, seizure of documents, etc. The relatively small number of requests for ML is explained by the fact that most of the requests are received for predicate offences, but in the course of their processing issues indirectly related to ML are also considered. In addition, a significant number of issues of mutual interest are resolved at the stage of information exchange through the FMA prior to a public investigation. Thus, there is every reason to believe that the county is able to provide effective and constructive assistance to both predicate offence requests and ML requests.

1140. The GPO has received MLA requests, including those requiring adjustments to international and domestic legislation for quality execution by law enforcement. In these instances, the GPO works with foreign counterparts to obtain the missing information required to properly execute the request and prepare a response (see Example 2.2)

Case Study 2.2 Requesting additional information from foreign competent authorities

On 07.02.2022, the GPO received a letter from the Prosecutor General's Office of the Republic of Moldova requesting consideration of a request for legal assistance in a criminal case. It is established that

the Prosecutor's Office for Combating Organized Crime and Special Cases of Moldova is investigating a criminal case against Kazakh and Moldovan citizens for extorting from A.S. his property (shares in companies). The request indicates that the case in Moldova is being investigated under Article 186 of the Criminal Code of Moldova, i.e. blackmail, and the Moldovan side requested materials of the existing criminal cases against A.S., procedural documents and decisions taken in these cases, as well as to identify and serve summons to the citizens of Kazakhstan. For qualitative fulfillment of the request, additional information was requested from Moldova, including materials of the Moldovan case, testimonies, etc., since the criminal legislation does not contain the article "blackmail"..

On 29.03.2022 a request was received from the GPO of Uzbekistan, which was sent as part of a criminal case under Article 228 (manufacture, forgery, documents, their sale or use) of the Criminal Code of Uzbekistan. However, from the content of the instruction it was not clear what the forgery or use of documents was, in what way and by whom, according to the investigation, this crime was committed. Besides, in points 2, 3 and 4 of the inquiry the initiator asked to interrogate the officials and drivers of the vehicles of the LLC K, F and T and to seize the documents related to the import of the agricultural products from the customs authority of the Republic of Kazakhstan. At the same time, it was not clear from the content of the order what relation these persons had to the crime under investigation, i.e. the request did not contain the grounds for the requested investigative actions, information about the crime committed or the damage caused as a result of sending goods by LLC K to the economic facilities located in the territory of the Republic of Kazakhstan. Moreover, the order on seizure of the bank information of the above-mentioned company from the National Bank was attached to the order. Meanwhile, the order itself did not contain a request to conduct the specified investigative actions. Also, the texts of the copies of customs declarations attached to the request were unreadable. As a result, a letter was sent to the GPO of Uzbekistan asking for additional documents and information needed to organize the execution of the assignment. After the deficiencies were corrected, the request was executed by the Kazakhstani law enforcement authorities.

1141. MLA requests are administered at the level of central apparatus of competent authorities. There are subdivisions (authorized employees), responsible for international cooperation, which control the process of responding to requests, in the GPOs, SCs as well as LEAs/SSAs. For example, in the GPO there is a specialized subdivision (Department of Extradition and International Legal Assistance of the International Legal Cooperation Service, consisting of 6 staff members). In addition, in the regional prosecutor's offices the relevant functions are performed by 23 authorized employees. A similar situation with human resources is observed in all competent authorities. Based on the number of annually considered requests and availability of authorized employees in the territorial bodies the resource provision of the competent authorities for quality and timely execution of international requests seems to be adequate.

1142. When MLA requests are received, they are checked for compliance with the requirements of international treaties, as well as with domestic legislation. It should be noted that dual criminalization, as well as literal conformity of names of criminal law norms are not grounds for refusing to provide MLA in cases when such assistance is not related to coercive measures. After verification of the incoming request, it is forwarded to the executor. Virtually all requests for MLA are executed, and substantive responses are given. After checking the received request, it is promptly transferred to the executor (investigator, inquirer).

1143. The system "Kadagalau" is used for transmission and distribution of requests received by the GPO, which is a system of office workflow, within which the control of execution of requests is provided. Initially, a deadline for execution is set for the executor in the GPO and in the case of a request sent to a territorial prosecutor's office or other body, it is manually set for the subsequent executor. Similar case management systems are available in all LEAs/SSAs. At the same time ML/TF requests are executed as a priority, which is stipulated in internal departmental orders of the GPO and all competent authorities.

1144. In the Republic of Kazakhstan there are no prohibitions or inappropriate and restrictive conditions in relation to the provision of MLA. From the legal point of view, refusal is possible if the requested assistance may harm the sovereignty, security, public order or other essential interests of Kazakhstan, which generally

complies with international legal standards, in particular subparagraph b of paragraph. 21 of art. 18 of the Palermo Convention. According to the statistics on refusals to execute MLA requests, the Republic of Kazakhstan has not refused requests for legal assistance on the grounds of the abovementioned reasons, as well as on the grounds that the crime is related to tax issues or on the grounds of secrecy or confidentiality requirements for financial institutions or DNFBPs. A total of 19 cases have been denied by Kazakhstan during the assessment period, and they do not relate to ML/TF cases.

1145. In general, the organization of the MLA system allows the competent authorities of the country to provide a significant amount of legal assistance in a short period of time – up to 3 months.

1146. According to the information provided during the on-site, all MLA requests incoming through the GPO are executed rather quickly, as a rule, from 1 to 3 months, which is confirmed by the statistics provided. No more than a quarter of incoming requests are executed within more than 3 months. Longer terms are isolated and related to complex cases, large volume of collected data and necessity to obtain additional information from the initiator of the request. The requests received by the MIA, FSA, NSC and ACA directly are executed almost in 100% of cases within 3 months. Thus, for example, the average time to reply to the inquiry considered by the FMA in 2021 made 28 days. Such rapidity of execution of requests is a convincing confirmation of the work of the system to provide the MLA.

1147. According to the information provided by the GPO, the MLA requests for search, seizure and return of assets have not been received. At the same time, the legislation of the Republic of Kazakhstan allows the implementation of relevant procedures, and the competent authorities have demonstrated understanding of the issue.

1148. According to the information provided by the GPO, there were no MLA requests for the return of assets from the Republic of Kazakhstan. Accordingly, there were no facts of return of assets from the Republic of Kazakhstan to other jurisdictions, however, there was a fact of seizure of assets at the request of the competent authorities of Denmark, which was subsequently cancelled at the request of the initiator. The small law enforcement experience in the field of search and seizure of assets at the request of the MLA nevertheless did not affect the ability of the competent authorities of Kazakhstan to implement the relevant procedures, which was sufficiently demonstrated in the course of the on-site mission. To date, the SC and other competent authorities have not received requests related to the criminal use of cryptocurrencies and other virtual assets in ML and TF, therefore, given the existing cross-border risks in this area, measures should be taken to develop regulatory, organizational and methodological mechanisms for the execution of relevant requests (outside the IFCA). The SC executed 16 requests of foreign courts in criminal cases, including one AML/CFT request from Latvia (Example 2.3).

Case Study 2.3 Execution of request by SC

According to the court order, received by the Supreme Court through the Ministry of Justice of the Republic of Kazakhstan, in the proceedings of the Court of Vidzeme suburb of Riga was considered the trial of property obtained by criminal means, on the decision of the investigator of the Office for Combating Economic Crimes of the State Police of the Ministry of Interior of the Republic of Latvia.

The order for service of court documents stated the requirement to serve a court summons on RK citizen B. to participate in a pretrial criminal proceeding.

In Kazakhstan, citizen B. was found guilty of committing crimes under part 3 of article 28, paragraph 2 of part 4 of article 189 of the Criminal Code and sentenced to 8 years of prison with confiscation of property and deprivation of the right to engage in banking and financial activities associated with financial responsibility for 10 years, and he is currently serving his sentence.

The Latvian party knows that B. is convicted in Kazakhstan and is serving his sentence in the facility, as in its request, it indicated the address of the facility to send the order to.

On September 02, 2021, the institution of the Department of the Criminal Executive System of the city

of Almaty executed the court order, and the documents were handed over to convict B.

The judicial authority sent the executed court order to the Ministry of Foreign Affairs.

The Latvian side was satisfied with the execution of the request, about which feedback was requested.

1149. Based on the information presented during the on-site mission, significant attention is paid to the issues of training and professional development of staff involved in ensuring international cooperation, both through intradepartmental training (various methodological manuals on the procedure for sending MLA requests, procedures for asset recovery from abroad were published by the GPO), and advanced training in educational institutions and international organizations.

1150. Professional development of the staff of units involved in international cooperation is carried out both within the framework of training programs of the Academy of Law Enforcement Agencies under the GPO, and through the projects and activities of international organizations (UNODC, World Bank, CARIN, LEICA, GRECO, etc.). At the same time, a significant number of training events address ML/TF related issues, ranging from general procedural issues to their substantive content (Table 2.6). The data provided by the country shows that there is a sufficient level of training and staff development in international ML/TF cooperation, which was generally evident during the on-site mission.

Table 2.6. Number of training events that addressed international cooperation on ML/TF

Authority	2017	2018	2019	2020	2021	Total
GPO	10	15	23	12	15	75
FMA	7	6	11	5	17	46
MIA	5	8	15	4	7	39
ACA	12	16	18	7	12	65
NSC	4	7	13	3	5	32

Extradition

1151. From 2017 to 2021. The Republic of Kazakhstan received 565 extradition requests for different types of criminal cases. There were no extradition requests for ML/TF. The requests for extradition concerned crimes against persons (81), against property (277), economic activity (7), corruption (8), terrorist and extremist activity (18), illigal drug trafficking (37), human trafficking (18) and other crimes (illegal border crossing, traffic accidents, self-law enforcement, etc.). No ML/TF requests for extradition were received

Table 2.7. Provision of legal assistance requests on criminal extradition via the GPO

	2017	2018	2019	2020	2021	1st half 2022
Incoming requests	110	134	131	74	71	45
Executed extradition requests	104	101	117	64	62	39
Refused	6	11	14	10	9	6

1152. The country refused 56 requests from foreign states for the extradition of wanted persons. The reasons for refusals are related to expiration of the statute of limitations for criminal prosecution (46.4%), for crimes that do not pose a great public danger and are not predicate offenses (30.1%), if the wanted person has Kazakh citizenship (10%), if the wanted person is extradited to another state (5.3%), if it is legally impossible, that is, if asylum is granted (5.3%), if the same crime has been committed (3.3%).

1153. Thus, the Kazakhstan does not deny extradition on unreasonable grounds and generally cooperates effectively in the extradition of criminals and most of the relevant incoming requests are granted.

8.2.2. Submission of requests on operative mutual legal assistance with domestic ML-related cases,

predicate offenses, and transnational FT

Mutual Legal Assistance

1154. The competent authorities in Kazakhstan are well aware of the risks outlined in the NRA, and seek to appropriately address the transnational element of crime where it can be identified, including through the mechanisms of the MLA.

1155. The FATF Global Network survey reported a single case of poor quality request preparation by Kazakhstan, which represents 0.1% of the total number of requests. At the same time the examples and statistics provided by the country, as well as other feedback from the FATF Global Network members testify to the positive experience of MLA provision in the Republic of Kazakhstan. In this regard, the presence of one negative feedback cannot be evidence of systemic problems in the organization of requests for timely provision of MLA and is rather an exception, which cannot affect the overall assessment of this criterion.

1156. A significant proportion of the requests initiated by the competent authorities of Kazakhstan are for predicate offenses The majority of such requests are made through the GPO, with a slightly smaller number made directly by the MIA and other LEAs/SSAs.

Table 2.8. Number or MLA requests submitted by Kazakhstan via the GPO

			2017	2018	2019	2020	2021	2022 (6 mnths)	Total
Sent			636	667	434	163	240	91	2231
On ML			*9*	*29*	*23*	*21*	*35*	*6*	*123*
On BO			*0*	*14*	*8*	*0*	*20*	*0*	*42*
Refused to be executed by foreign states			9	5	3	0	0	0	17
On ML/TF issues			*0*	*0*	*0*	*0*	*0*	*0*	*0*
Requests sent to a foreign states									
Total sent			636	667	434	163	240	91	2231
By authorities	**Regional prosecutors' departments**		610	639	355	138	213	77	2032
		Regional offices of EIS	*95*	*67*	*47*	*19*	*24*	*15*	*267*
		Regional offices of MIA	*422*	*511*	*265*	*86*	*149*	*51*	*1484*
		Regional offices ACA	*58*	*32*	*24*	*17*	*22*	*7*	*160*
		Regional offices NSC	*35*	*29*	*19*	*16*	*18*	*4*	*121*
	Central department of MIA		3	10	16	10	11	9	59
	Central department of ACA		5	10	44	12	13	1	85
	Central department of NSC		12	6	6	3	2	3	32
	Central department of MIA		6	2	13	0	1	1	23
LEAs/SSAs requests executed by foreign states									
Total requests executed			598	612	393	125	201	73	2002
Requests sent by	Regional prosecutors' departments		573	586	318	102	176	59	1814
	Central department of MIA		3	9	17	9	10	9	57
	Central department of ACA		5	9	40	11	12	1	78
	Central department of NSC		11	6	6	3	2	3	31
	Central department of MIA		6	2	12	0	1	1	22
LEAs/SSAs requests executed by foreign states on ML/TF issues									
Total executed			*9*	*29*	*23*	*21*	*33*	*4*	*119*

Table 2.9 Total requests sent by EIS

		2019	2020	2021	2022 (6 mnths.)	Total
	Sent	78	85	97	79	339
	Executed	58	64	73	26	221
	Refused	8	11	9	0	28
	On ML/TF	0	0	0	0	0

Table 2.10 Total requests sent by MIA

		2019	2020	2021	2022 (6 mnths.)	Total
	Sent	270	388	515	171	1344
	Executed	270	388	515	171	1344
	Refused	0	0	0	0	0
	On ML/TF	0	0	0	0	0

Table 2.11 Total requests sent by ACA

		2019	2020	2021	2022 (6 mnths.)	Total
	Sent	9	28	12	20	69
	Executed	9	21	6	5	41
	Refused	0	0	0	0	0
	On ML/TF	0	0	0	0	0

Table 2.12 Total requests sent by NSC

		2019	2020	2021	2022 (6 mnths.)	Total
	Sent	64	51	90	20	225
	Executed	62	47	77	13	199
	Refused	1	0	0	0	1
	On ML/TF	0	0	0	0	0

1157. According to the information provided by the country, the LEAs/SSAs sent MLA requests in the following categories of crimes: against property (fraud, theft, embezzlement, including budget funds, etc.) - 32.9% of the total number of requests, in the sphere of economic activity (tax evasion, economic smuggling, etc.) - 18.9%. Corruption (except budget misappropriation and embezzlement) - 8.5 %, terrorism and extremism - 2.3 %t, drug trafficking - 3.6 percent, against the person (murder, rape, bodily harm, etc.) - 22.7 % and others - 11.1 %. This indicates that the country's profile of predicate crimes is consistent.

1158. Among the countries to which requests were most frequently sent were: Russia - 961, Uzbekistan - 156, Turkey - 135, China - 99, UAE - 97, Germany - 77, Ukraine - 74, UK - 65, USA - 57. The specified countries as a whole correspond to economic relations of Kazakhstan.

1159. A total of 123 MLA requests were sent by the competent authorities of the Republic of Kazakhstan during the period under review. The majority of such requests are related to the investigation of criminal cases investigated on theft of property, corruption crimes, tax evasion and fraud. Statistical data and the content of MLA requests indicate that they are in line with the country's profile of predicate offenses.

1160. During the reporting period, it was mainly the CSI (28 refusals, see Table 2.9) that received refusals on MLA. This was due to incorrectly worded requests. The rejected requests were analyzed, and training sessions were held with the staff, including with the participation of international experts. The result of this work was improved understanding, which led to more competent drafting of requests and absence of refusals in the first half of 2022.

1161. There were 6 TF requests during the reporting period (1 in 2018, 2 in 2019, 2 in 2020, 1 in 2021). The requests were sent mainly to Turkey, which corresponds to the risk profile of the country.

1162. The SC sent 6 requests for predicate offenses, and there were no ML/TF requests.

1163. The record of the requests for legal assistance sent by GPO to foreign countries, as well as those received from foreign countries, is kept through the posting of statistical cards in the system "Kadagalau", there is also established a corresponding control, which was clearly demonstrated to the team during the on-site mission and demonstrates the proper control over the progress and results of the execution of requests sent to foreign jurisdictions.

1164. LEAs/SSAs make efforts to identify, seize and confiscate assets abroad, which, among other things, is facilitated by the implementation of the Stolen Asset Recovery project in the Republic of Kazakhstan since 2016. Alternative formats of international cooperation are used, including CARIN, ARIN AP, ARIN-

WCA, INTERPOL FOCAL POINT and others. Several successful requests were made to Switzerland, Belarus, and Latvia during the period under assessment regarding the confiscation of large amounts related to ML, money laundering, and theft of assets (Example 2.4-2.6). Thus, statistical information indicates that MLA is actively and effectively used by the MLA in the search for and recovery of criminal assets abroad

Case Study 2.4 Requests to identify, seize and confiscate criminal assets

FMA was investigating a criminal case against K., who in 2019 in conspiracy with officials of a national company organized the theft of its funds in the amount of 14.5 billion KZT in the import of foreign gas through an intermediary firm LLP "A". Subsequently, the stolen money was illegally legalized by accruing dividends to the founders of LLP "A" and distributed among the participants in the crime. Also, K. is accused of embezzlement of funds of the national company by selling gas for export at a price below the market price to the foreign affiliated companies of K., which was resold to European countries. As part of a parallel financial investigation, it was found that the stolen funds received from gas exports were transferred to the accounts of foreign companies, where the beneficial owner was K. Subsequently, illegally obtained profits were legalized in the form of investments in business projects in the Republic of Kazakhstan and abroad. In the course of the financial investigation the property of the persons involved was established and seized for a total of 42.2 billion KZT. At the same time, the investigative authorities, based on information received from foreign FIUs, sent international investigative orders to identify, arrest and confiscate the criminal assets of the suspects.

Case Study 2.5 Asset recovery from Switzerland

In the course of an investigation, it was established that between 2007 and 2009, K. and others created a criminal association to illegally move goods from China across the customs border of Kazakhstan. These persons passed the proceeds of crime to citizen A. to launder and transfer assets abroad. At the same time, A. in order to launder criminal assets on the basis of sham contracts transferred outside the Republic of Kazakhstan monetary assets to the accounts of foreign companies opened by him in banks in Switzerland. Having established the location of criminal assets, the GPO sent a request to Switzerland to seize the accounts and return the funds to the Republic of Kazakhstan. As a result of close cooperation between 2017 and 2020, Swiss federal authorities returned $1.3 million in criminal assets to the RK. The verdict of the Almaty court sentenced the members of the criminal association to various forms of punishment with confiscation of property.

Case Study 2.6 Request for prosecution

In 2016, during the interrogation of one of the members of the organized criminal group A., investigators learned the name of his accomplice, who created a network of one-day firms, through which money stolen by A. (a bank official) from the bank was laundered. According to the information received, the named person was operating in the territory of the UAE, and a request for legal assistance was sent to the said jurisdiction.

Through cooperation with UAE law enforcement authorities, it was possible to obtain incriminating evidence and supporting documents against A. and his associates.

Their analysis revealed that A. continued to be the owner of a large asset in Kazakhstan, which was managed from the United Kingdom.

The aggrieved party exercised its right to see the documents and brought an action against A. and his accomplices in the High Court in London, which at that time had already ruled to recover from A. the $4 billion in funds stolen by him from the Bank.

As a result, the UK court ordered the recovery of the assets in question, worth about $500 million, in

favor of the aggrieved party. The investigation also revealed that A. had purchased the asset with the funds stolen from the Bank.

A. subsequently sold part of his interest in the asset and invested the money to purchase real estate in the United States. The aggrieved party filed a civil lawsuit in the United States against A. and his associates for laundering the stolen money.

The difficulty in proving A.'s connection with the asset was that the ownership was hidden behind a chain of one-day firms registered in various offshore jurisdictions.

As a result of the analysis of documents received from the UAE, the investigators found that these companies were managed by a registrar firm registered in the Isle of Man. Maine.

The investigation prepared and sent an international investigative assignment to the Isle of Man. As a result of cooperation with the competent authorities of that jurisdiction, evidence was obtained that A. secretly remained the owner of the asset in Kazakhstan and that the asset itself had been purchased with the stolen funds from the bank.

As a result, the obtained documents served as evidence in the American court, where the jury awarded the injured party B Bank JSC damages in the amount of 100 million US dollars with interest accrued since 2013, the total amount of the verdict was 218 million US dollars.

Extradition

1165. The GPO has a central role when requesting the extradition of a person at the request of the competent authorities of foreign states, as the prosecutor examines the criminal case file, verifying the legality and validity of its initiation, the adoption of procedural decisions regarding the person sought for extradition, preparing an opinion on the validity of the request sent, as well as the request itself.

1166. The right to initiate an extradition arrest before a court also belongs to the prosecutor, who is obliged to question the detained person, to verify information about his being on the international wanted list, his status of accused or convicted person, the application of a preventive measure of arrest against him, his citizenship, and also to make sure that the punishment provided by law for the crime committed is over 1 year or the unserved part of the sentence is over 6 months.

1167. International agreements and the CPC do not provide for the application of extradition arrest to own citizens, suspects, as well as those who are on the national wanted list, who have been given a measure of restraint in the form of a written pledge not to leave the country.

1168. During the evaluation period, 432 requests for legal assistance for extradition were made, including 6 ML requests (see example 2.7). No legal assistance for TF was requested. The statistics of extradition requests are as follows: for crimes against property (fraud, theft, embezzlement, etc.) - 54% of the total number of requests, in the sphere of economic activity (tax evasion, economic smuggling, etc.) - 6%. The other crimes against individuals (murder, rape, bodily injury, etc.) made up 18.7%; terrorism and extremism, 2%; drug trafficking, 7.5%; and others, 10.1%.

Table 2.13. Legal assistance requests on the extradition of criminals by the GPO

	2017	2018	2019	2020	2021	2022 (6 mnths)	Total
Sent requests	109	101	80	54	56	32	432
Executed requests for extradition	62	70	63	56	34	28	313
Refused	13	11	7	5	5	4	45
On ML	0	0	0	0	0	0	0

Case study2.7 Extradition on ML

Since 2015, the competent authorities of the Republic of Kazakhstan have been investigating a criminal case involving the theft of funds and laundering of criminal proceeds in the amount of USD 7.5 billion.

One of the defendants in this case was citizen T., who was suspected of complicity in the theft and laundering of assets of a Kazakhstani bank in the amount of more than 1.5 billion U.S. dollars. Citizen T., who was involved in this crime, was detained on the territory of the Republic of Uzbekistan, in connection with which a request for his extradition was sent to the Prosecutor General's Office of the Republic of Uzbekistan in December 2018. Based on the request, the Prosecutor General's Office of the Republic of Uzbekistan extradited citizen T. to the Republic of Kazakhstan. In 2019, citizen T. was convicted and sentenced by a court verdict in Almaty.

1169. According to statistics for the period 2017-2022, there were no refusals of extradition in ML cases. However, there is an example, when for a predicate offence in 2014 France refused to extradite Gr. After that, in 2017, materials were sent to initiate criminal proceedings in France. Based on the results of the consideration of the materials, a criminal case was initiated, which is currently being investigated by the investigating court in Paris. A similar practice of referring cases for prosecution is carried out for other categories of crimes. At the same time, work on the voluntary return of wanted persons on refusals of extradition is carried out. During this period, as a result of the explanatory work carried out by the LEAs/SSAs, 10 persons for whom extradition was refused by foreign competent authorities were voluntarily returned to the country. These examples demonstrate that there is alternative practice in Kazakhstan in cases where foreign jurisdictions refuse to extradite individuals (see examples 2.8-2.10).

Case Study 2.8 On fugitives

In 2009, a criminal case was opened regarding the theft and laundering of assets of JSC B Bank by citizen A., who fled from the investigation and was put on the international wanted list. In 2013, through the channels of Interpol, A. was detained in France. At the same time, the GPO sent a request for extradition to the French Ministry of Justice. In 2014, French authorities refused to extradite A. to Kazakhstan due to the absence of an extradition treaty, in connection with which the GPO appealed to the French law enforcement authorities to initiate criminal proceedings against A. on the basis of the international principle of "extradite or prosecute", i.e. for crimes committed in Kazakhstan. In 2017, based on the materials sent by the GPO, the Prosecutor's Office of Paris opened a criminal case against A. for the theft and laundering of 1.2 billion US dollars. In 2020, A. was found by an investigative court in Paris to be a suspect in breach of trust and money laundering. Seizure, confiscation and recovery of assets are underway.

Case study 2.9 On persons refused to be extradited

In the case of JSC "B Bank" a member of the criminal community, citizen of the Republic of Kazakhstan Zh. escaped from the investigation authorities. As a result of her criminal activities JSC "B Bank" incurred material damage totaling 700 billion KZT. Through the channels of Interpol, she was identified and detained in Hungary, which refused to extradite Zh. in connection with the granting of asylum. As a result of explanatory work in 2017. Zh. voluntarily returned to the Republic of Kazakhstan. During the investigation, Zh. fully admitted her guilt in the incriminated crimes, disclosed details, and identified other accomplices of the criminal offence. In 2019, the verdict of the Almaty court found Zh. guilty of aiding and abetting the theft of another's property entrusted to the perpetrator, with the use of official position, on a large scale. Overall, as a result of the measures taken in this criminal case, 10 participants of the criminal association returned voluntarily.

Case Study 2.10 On prosecuting the persons refused in extradition

The NSC is investigated a criminal case against A. M. M. suspected of committing acts aimed at inciting

religious hatred, propaganda of terrorism, as well as participation in the activities of a terrorist group. Due to the fact that A. M. M. fled from the investigating authorities, on 03.02.2016 he was put on the wanted list and on 22.02.2016 the court sanctioned a preventive measure in the form of detention against him. Through the channels of Interpol, information was received about the residence of A. M.M. on the territory of the Republic of Austria, using the passport of a Russian citizen. On 25.09.2018, the GP sent a request for the extradition of A.M.M. for criminal prosecution. According to the note verbale of the Federal Ministry of Europe, Integration and International Affairs, the criminal court of Vienna on 17.10.2018 refused to extradite A.M.M. Despite the refusal to extradite GOP took steps to prosecute him. At the same time, on 03.12.2021 the Austrian authorities reported that according to the materials submitted by the GP, A.M.M. was sentenced in Vienna to imprisonment for a term of 12 years.

8.2.3. Submission and receipt of requests and provision of other assistance in the context of international cooperation for AML/CFT

FMA

1170. The FMA represents the interests of the Republic of Kazakhstan in international organizations in relation to AML/CFT, is authorized to exchange AML/CFT-related information, details, and documents with competent authorities of other countries on request or proactively, make correspondent agreements, and communicate with them to identify people, organizations, and beneficial owners involved in ML/TF as well as to trace the money and/or other property belonging to such persons. The FMA established contact with the FIUs of more than 160 foreign countries through the Egmont Secure Web. The FMA has been a member of the Egmont Group since 2011 and works together with foreign FIUs, both members and non-members of the Egmont Group, has been taking active part in EAG events since 2004, and has been a part of the CIS Council of FIU Heads since 2012. In order to establish a legal framework for and extension of interdepartmental collaboration with the competent authorities of foreign countries, the FMA initiated and signed 41 agreements and memorandums of cooperation, including Ukraine, Moldova, UAE, Russia, Belarus, Kyrgyzstan, Tajikistan, China, Cyprus, Macedonia, Montenegro, Turkey, Romania, Lithuania, Japan, Croatia, Armenia, Poland, Panama, Bangladesh, Georgia, Mongolia, Korea, Israel, UK, Serbia, Canada, Latvia, Hungary, Uzbekistan, Turkmenistan, Afghanistan, India, Albania, Pakistan, Macao, Togo. And with AFCA and BN KZ Technologies Limited.

1171. If the financial monitoring gives reasons to suspect money laundering, predicate offenses or financing of terrorism in relation to subjects of foreign countries or transactions with foreign countries, the FIU prepares and submits a request to the FIU of a corresponding country.

1172. A request is prepared and sent as a matter of priority if it relates to terrorist financing or very high and high risk offenses as defined by the NRA. FMAsystematically request information from foreign FIUs when conducting financial investigations with a foreign component. The intensity of requests varies, but generally remains at the same level, indicating a stable level of use of these channels to obtain the necessary information.

Table 2.14. Requests and messages submitted to the FIUs of foreign countries

	2017	2018	2019	2020	2021	6 mts 2022
Outgoing requests	**143**	**126**	**119**	**273**	**363**	**325**
including those submitted on authorized requests from the LEA and SSAs						
NSC	4	-	5	9	15	164
ACA	2	2	2	24	6	5
EIS	60	6	8	61	44	22
MFA	1	-	6	23	15	0
GPO	4	3	0	0	0	1
including those connected with suspicion in:						
Embezzlement of public funds	11	29	46	113	228	123
Tax crimes	82	42	22	92	46	7
Fraud (incl. pyramid scams)	7	1	17	9	33	3

Corruption offenses	-	3	3	33	9	1
Illegal drag trafficking	5	9	5	5	5	4
Underground economy	-	-	-	8	12	-
Financing of terrorism	38	38	26	12	22	23
Other	-	4	-	1	8	164
including those with requests for:						
Information on beneficial owners	95	76	86	225	324	295
Average response time (in days)	48	35	36	42	30	30
Materials provided to foreign partners proactively	-	10	36	11	12	-

1173. 80% of outgoing requests from the Kazakhstan were related to the identification of beneficial owners, while in practice there were no cases of refusal to provide information.

Table 2.15. Number of international requests submitted to FIUs

YEAR	ML	TF
2017	105	38
2018	88	38
2019	93	26
2020	261	12
2021	341	22
2022	302	23
Total	1190	159

1174. As can be seen from the table above, after 2019, there is an increase in the number of requests sent, which is explained by the fact that in 2019 the structure of the FMA was changed by joining the FIU and the EIS, thereby increasing the number of analysts and creating an additional analytical department engaged in tactical analysis. In addition, this change has had a positive impact on improving interaction with all of the LEAs, especially with the EIS, which is a key body for investigating cases involving economic crimes. Thus, the agency's structural changes have had a positive impact on the level of international ML/TF cooperation.

1175. The most active exchange of information for the period 2017-2022 corresponds to the directions of financial flows of the Republic of Kazakhstan, reflecting the directions of export-import and was carried out with the FIUs of Russia, the UAE, Turkey.

1176. All the law enforcement agencies are aware of the FMA's capabilities with regard to international cooperation with foreign FIUs, and use the opportunities for exchange of information wherever needed. However, the FMA EIS uses the FIU's authorities in this field most of all which implies efficiency of the structure and the FMA's authorities for investigation of ML or other economical crimes. Other law enforcement agencies use the FIU's resources to a lesser extent.

Table 2.16. Requests received by the FMA from FIUs of foreign countries

	2017	2018	2019	2020	2021	6 mts 2022
Incoming requests	**115**	**114**	**127**	**148**	**78**	**60**
including those connected with suspicion in:						
ML	66	91	83	118	51	34
Tax crimes	16	8	11	4	2	6
Embezzlement of public funds	10	3	4	2	5	2
Fraud	-	-	9	3	4	3
Illegal drag trafficking	2	-	5	6	1	1
Corruption offenses	1	2	7	3	1	-
FT	20	10	6	12	13	14
Underground economy	-	-	2	-	1	-
including those with requests for:						
Information on beneficial owners	66	54	75	59	68	50

Average response time (in days)	42	38	32	34	28	30
Proactive materials	44	61	47	51	67	24

1177. All of the inquiries sent contained questions about the registration data of foreign individuals, the existence of bank accounts, the movement of funds through them, as well as the presence of movable and immovable property and other assets. All "follow the money" analyses and investigations tracked the ultimate beneficiaries of the funds.

Case Study 2.11 Use of information received on an TF-related request

In 2022, a joint investigation was made by the FIU FMA, the FIU of Turkey, the Russian Federation, and the National Security Committee of the Republic of Kazakhstan against Mr. A involved in financing of terrorism.

According to the information provided by the Russian Federation, in November 2021 a Russian citizen U against whom a criminal case was initiated under Article 205.1, clause 1.1 of the Criminal Code of the Russian Federation (Inducement, recruitment or other involvement of a person in support of terrorist activities) transferred 500 US dollars through Zolotaya Korona payment system (without opening an account) to Turkey in the name of Mr. A, a Kazakh citizen.

It was used as a reason to perform detailed financial monitoring together with foreign FIUs and the law enforcement agencies of our country.

During the detailed monitoring, 11 STRs from K BANK were examined and it was found that Mr. A provided regular financial support to his counterparts Sh and S (citizens of the Republic of Kazakhstan) and accompanied his wrongful intents in mass media with propaganda and exhortations to commit acts of terrorism.

To implement his ideas, he transferred more than 440 thousand KZT to his counterparts during the period since September 2021 till February 2022 on a non-reimbursable basis.

The total cash flow though the accounts belonging to Mr. Sh and Mr. S for 2021 was more than 400 million KZT while those persons had no official jobs according to the database of the Unified Pension Savings Fund.

Communication with foreign FIUs helped to confirm involvement of the involvement of Mr. A in terrorist activities in a short time.

As a result of the inspections, the NSC of the Republic of Kazakhstan initiated a criminal case against Mr. A under Article 256, part 2 of the Penal Code of the Republic of Kazakhstan (propaganda of terrorism or public calls for commission of an act of terrorism).

On July 26, 2022, Mr. A was found guilty in a crime of terrorism by Al-Farabi district court of Shymkent city with regard to case 5211-2200-1/316, imprisoned for 7 years, and, on July 27, 2022, included into the FT sanctions list in virtue of which urgent freezing measures were taken.

Mr. Sh and Mr. S have been subjected to inspection activities.

Case Study 2.12 Use of the information received from foreign partners by the FIU

In March 2021, the Austrian FIU received spontaneous information on an individual entrepreneur from Kazakhstan who transferred large amounts of money to Austria as a payment for goods. The FIU FMA performed a tactic analysis, including examination of bank account statements, foreign exchange contracts, and external economic activity. It identified 7 interlinked individual entrepreneurs who systematically deposited to bank accounts and transferred abroad more than 1 billion US dollars. Analysis revealed that contracts were made between sellers from Uzbekistan and buyers from Kazakhstan. Contracts were made for supply of fruits and vegetables to Kazakhstan on condition of 100% initial

installment. After that, he parties concluded additional agreements to the contract to amend the clause which obliged the buyer to pay for the supplied good on behalf of a third party. For example, a third party to the contract between OOO R (Uzbekistan) and IP A (Kazakhstan) was a Chinese company which supplied textile products of OOO R. Also, as a part of an additional agreement, the parties added a clause to the contract wherein they specified that the buyer shall pay for the goods supplied for the seller on behalf of the third party OOO M (Russia). Under the contract between OOO R and OOO M, OOO M supplies metals to OOO R. Changes to the contract in relation to payments to third parties were initiated by OOO R (Uzbekistan) which imported textile products from China and metals from Russian to Uzbekistan. The goods were imported under contracts made with suppliers, and OOO R is responsible/liable for making payments. On the other hand, IP A has payment obligations under the contract with OOO R. In April 2021, analysis findings were submitted to the EIS. The EIS initiated criminal cases on the ground of clause 235 of the CC of the Republic of Kazakhstan (Non-fulfillment of the requirement of repatriation of national and/or foreign currency). It was established that a few Uzbekistan citizens and 2 Kazakhstan citizens arranged withdrawal of funds from Kazakhstan to foreign countries.

The funds were transferred with the use of the details of 7 individuals unrelated to foreign trade transactions. Ultimate beneficiaries of the international money transfers were Uzbekistan entrepreneurs, and Uzbekistan companies were specified as recipients of goods in invoices. The principal reason for money transfer from the Republic of Kazakhstan were low commission rates (0.1% while rates for transfers through Uzbek banks were up to 1%). At the same time a group of Uzbek entrepreneurs presumably exported goods (mostly fruits and vegetables) to the Republic of Kazakhstan and Russia, and sales proceeds (mostly cash from sales in markets) were accumulated in the Republic of Kazakhstan and transferred to third parties as requested by the Uzbek entrepreneurs. The authorities also managed to identify those who played certain roles in the group, including the organizer's assistant who found people to control the process of money transfer, people who deposited money to bank accounts, people who translated chats from Uzbek, the person who provide technical support to the internet banking system, the person responsible for accounting and bank accounting, the representative in public authorities, and the lawyer.

Case Study 2.13 Use of spontaneous information from the FMA by foreign partners

In December 2020, the FIU FMA submitted provided the FIU of the Russian Federation with spontaneous information on one individual and two legal entities from the Russian Federation having mutual settlements with a Kazakh company, including the following details. The analysis revealed that a Russian citizen D was involved in suspicious activity connected with possible risks of tax evasion. Mr. D was the leader/founder of TOO O. The main buyer of TOO O was OOO F; and there were also insignificant mutual settlements with OOO N. Goods were supplied to the Russian Federation during the period since 2016 till 2017. According to the information posted on the web-site SPARK (information analysis system), OOO F and OOO N has registered office at one and the same address. Also, according to SPARK, Mr. D was the leader of OOO F which implies affiliation between TOO O and OOO F which could play a certain role in bilateral mutual settlements. At the present moment, TOO O is acknowledged by the national revenue authority as an inactive taxpayer and taken off the register due to its absence at its registered location. Taking into account the fact that the Russian citizen established a business enterprise in the territory of the Republic of Kazakhstan, purchased goods in the territory of the Russian Federation, and effected deliveries to its affiliated companies, there are reasons to doubt the economic feasibility of transactions. At the same time, a permission was provided to transfer the requested information to the Russian law enforcement agencies as well as to the involved foreign FIUs solely for the purposes of investigation.

In response, the FIU of the Russian Federation informed that screening activities were being performed together with the Russian customs authorities in relation to Russian company OOO F, and its director

and founder Mr. D.

According to the received information, Mr. D performed illegal banking transactions for the transfer of funds through accounts of associated company in credit institutions located both on the Russian Federation and in the Republic of Kazakhstan (article 193.1 of the Criminal Code of the Russian Federation–currency transactions for the transfer of funds in foreign currency or the currency of the Russian Federation to the accounts of non-residents using forged documents). Also the FIU of the Russian Federation established that in 2017 Mr. D transferred more than 110 million rubles in total on behalf of OOO O to a controlled non-resident company under the contract with TOO O. During the period from August 17, 2017 till December 21, 2017, goods for an overall amount of more than 60 million rubles were received for the payments to OOO F. The transaction certificate was closed in October 2019 under clause 6.7 of Bank of Russia Instruction No. 181-I dated August 16, 2017. The amount of the fund subject to repatriation was about 50 million rubles.

Case Study 2.14 International cooperation for identification of a beneficial owner

On January 2020, a request from Rosfinmonitoring was received which informed that together with the FIU of Italy they were conducting an inspection of a Russian citizen for her possible involvement in laundering of incomes from criminal activities (a similar response was received from the FIU of Italy). During the period since September till October 2018, the Russian citizen received transfers from Kazakhstan accounts of foreign companies A and S in JSC SB Alfa Bank to the total amount of 500 thousand Euro and 2.58 million Euro respectively in the form of special-purpose loans.

In February 2019, the Russian citizen used the transferred funds to buy a house in Italy for more than 3 million Euro even though it was bought by the previous owner for 4.2 million Euro. It was supposed that a third party might be involved in the transaction. The FIUs requested information on the source of the funds transferred from Kazakhstan accounts of companies A and S to the subject of the request as well as information on the founders, managers, beneficial owners, and account administrators of companies A and S. Analysts of the FIU FMA conducted a number of checks on the available informational databases and submitted a request to second-tier banks to obtain the bank statements of the subjects and information on the beneficial owners.

The following was revealed:

Information from the second-tier banks of the Republic of Kazakhstan help to identify beneficial owners of the specified bank accounts who turned to be the citizens of the Russian Federation (full information on the owners was provided). The identified beneficial owners of the specified accounts of company C were the same citizens of the Russian Federation. Also, full information on the leader of the company was provided and it was specified that he was a founder of two more companies on Cyprus (and brief profiles of the companies were provided). Analysts identified the sources of the funds. Companies A and S conducted no business activities in the RK. They only used the services of Internet banking. Neither had any branches or offices in the territory of the RK. No information was found in the information systems on the property or pension contributions of the specified person nor any information on their being brought to civil or criminal liability. Those individuals made transactions as they took loans from each other and then transferred the full amount or its significant part with or without conversion into a foreign currency within one or more operating days to non-residents of the RK, mostly to offshore jurisdictions. In loan agreements, both the lender and the borrower were investment and consulting company B. It was managed by the same citizens of the Russian Federation as were the managers of the above-mentioned companies. The FIU FMA replied to the FIU of the Russian Federation on March 5, 2020, provided the requested information, and attached a scheme of movement of the subjects' funds.

1178. All of submitted requests include the details required for identification of the person in charge which may be later used to make a contact and clarify any necessary issues. Presence of corresponding details is

required by the established forms for exchange of information through the channels of Egmont Group.

1179. As required by the governing documents of the Egmont Group, as soon as an international request is registered by the FIU FMA, a notice shall be sent to the request initiator with confirmation of the request receipt, registration number, and contact details of the person in charge of execution of the request.

1180. There were no refusals to provide information through the channels of the Egmont Group. In some cases a meaningful response was not provided as the subjects of the request were not connected with the country the request was submitted to, and a request was submitted in return to clarify the reasons for the request.

1181. As for provision of spontaneous information through FIUs, it is provided less extensively. Meanwhile, it shall be noted that the Republic of Kazakhstan obtains much more spontaneous information than it provides which may confirm the risks of usage of transnational schemes by the residents of the RK and implies the necessity to promote international exchange of information. No spontaneous information was provided in relation to TF.

Table 2.17. Statistics on spontaneous information in the line of the FIUs

Year	Submitted	Received
	ML	ML
2017	-	31
2018	10	57
2019	6	42
2020	11	41
2021	5	58
2022	-	22
Total	32	251

1182. The geography of provision of spontaneous information is generally similar to that of the requests which is also connected with both the directions of cash flows and the risks of ML in general. They are mostly connected with dubious financial transactions.

1183. The information received by the Secretariat in relation to international cooperation between such jurisdictions as Belgium, Federal Republic of Germany, Hong Kong (the People's Republic of China), Macau (the People's Republic of China), Russian Federation, and Sweden demonstrates positive experience of interactions with the FIU of the Republic of Kazakhstan. The requests received are executed in time which among other things is supported by the fact that the FMA is a law enforcement agency. As the same time, the FIU of Belgium informed that 2 requests (to clarify the issue of correct understanding of the request and to provide additional information on supposed financing of terrorism) were not responded. At the same time, these single facts cannot be evidence of the systemic nature of the violations and do not affect the overall conclusion about a fairly good level of interaction between the FMA and foreign partners.

1184. In the context of fulfilment of FATF Recommendations 36 and 37 and cooperation with foreign law enforcement agencies of criminal investigations, the Service submitted 464 international investigation requests. Of them, 321 were executed and 143 are in the process of execution. In order to arrest property abroad with the total cost of 54 billion KZT (funds on bank accounts involved in 5 cases and 61 items of immovable property involved in 4 cases), 22 investigation requests were submitted to 12 countries (Russian Federation, Latvian, Czech and Austrian Republics, UAE, Swiss Confederation, Luxembourg, Slovakia, Estonia, Armenia, Turkey, and the USA).

1185. The FIU FMA together with the foreign intelligence service of the NSC identified the properties belonging to suspects and their close relatives abroad with the total cost of 48 billion KZT.

1186. The court seized the property in question and sent international investigative orders for legal assistance, which are currently being executed.

1187. There was 112 requests for legal assistance from foreign law enforcement agencies, of which 107

(95.5%) were executed, 5 are under execution (4.5%). Two requests for seizure were received for an amount of $4.2 million, of which one was executed and one is under execution.

1188. When information is received from foreign FIUs, financial investigations are conducted and the results are used to send information to other foreign FIUs as well.

1189. It should be noted that during the on-site the Republic of Kazakhstan demonstrated successful examples of the effective use of incoming information, both in terms of requests and spontaneous information.

Law enforcement agencies

1190. LEA/SSAs use other forms of international cooperation and can effectively use them in their activities, including to exchange experience and train the employees, exchange up-to-date information with foreign counterparts, and obtain expert support for criminal cases. There are no refusals to execute requests under other forms of international cooperation.

Table 2.18 Other forms of international cooperation except MLA (EGMONT, ARIN, CARIN, INTERPOL etc). Requests received and executed

		2017	2018	2019	2020	2021	2022 (6 mnths)	Total
Received								
by	GPO	3	5	13	2	7	2	32
	FMA	115	114	127	148	78	60	642
	MIA	1311	1425	1275	1470	1258	1121	7865
	ACA	0	0	0	0	0	4	4
	NSC	0	0	0	0	0	0	0
Executed								
by	GPO	3	5	13	2	7	2	32
	FMA	115	114	127	148	78	60	642
	MIA	1311	1425	1275	1470	1258	1121	7865
	ACA	0	0	0	0	0	4	4
	NSC	0	0	0	0	0	0	0
Numbers on ML/TF								
by	GPO	3	5	13	2	7	2	32
	FMA	ML-95, TF-20	ML-104, TF-10	ML-121, TF-6	ML-136, TF-12	ML-65, TF-13	ML-46, TF-14	ML-567, TF-75
	MIA	0	0	0	0	0	0	0
	ACA	0	0	0	0	0	0	0
	NSC	0	0	0	0	0	0	0

Table 2.19. Other forms of international cooperation by request of foreign counterparts (EGMONT, ARIN, CARIN, INTERPOL, etc)

		2017	2018	2019	2020	2021	2022 (6 mnths)	Total
Sent								
by	GPO	2	7	5	5	5	3	27
	FMA	143	126	119	273	363	325	1 349
	MIA	1928	2138	2353	2555	1400	1160	11534
	ACA	26	19	10	20	11	8	94
	NSC	0	0	0	0	0	0	0
Executed								
	GPO	2	7	5	5	5	3	27
	FMA	143	126	119	273	363	281	1305

by	MIA	1928	2138	2351	2517	1356	1117	11407
	ACA	25	18	9	20	11	4	87
	NSC	0	0	0	0	0	0	0

Numbers on ML/TF								
by	GPO	2	7	5	5	5	3	27
	FMA	ML-105, TF-38	ML-88, TF-38	ML-93, TF-26	ML-261, TF-12	ML341, TF-22	ML-302, TF-23	ML-1190, TF-159
	MIA	0	0	0	0	0	0	0
	ACA	0	0	0	0	0	0	0
	NSC	0	0	0	0	0	0	0

1191. On the basis of the Ministry of Internal Affairs there is the Interpol National Central Bureau, through which law enforcement agencies receive information on databases for state registration of vehicles, checking foreign nationals and stateless persons when crossing the state border at checkpoints and when registering in the Republic of Kazakhstan for possible international wanted according to Interpol records, including stolen and lost passports.

1192. The National Central Bureau of Interpol interacts with the competent authorities of the Republic of Kazakhstan, subdivisions of the General Secretariat of the International Criminal Police Organization of Interpol, law enforcement agencies of Interpol member countries, and representatives of the competent authorities of foreign countries certified at diplomatic missions and consular establishments in the Republic of Kazakhstan on the matters of fighting international crimes.

1193. The National Central Bureau of Interpol works under the corresponding regulatory and departmental legal acts, and operates in accordance with Joint Decree No. 481 dated July 12, 2017 (GPO, Ministries of Finances, Defense, Foreign and Internal Affairs, ACA, FMA, SSA, NSC, and Supreme Court), “Interactions in case of adjudgment into the international arrest warrant, request execution and submission by the competent authorities of the Republic of Kazakhstan through Interpol, and processing of the requests by the national Central Bureau of Interpol in the Republic of Kazakhstan”.

1194. The Republic of Kazakhstan is a member of the International Criminal Police Organization of Interpol:

- Millennium for fighting organized crime
- Kalkan for fighting terrorism.

1195. During the reporting period, 214 requests were received through Interpol in connection with fighting terrorism, and all of them were executed. Usually, Besides, adjudgment into the international arrest warrant, foreign counterparts ask for assistance with obtainment of underlying information, screening of individuals, legal entities, and their documents (authentic or lost), crossing the borders, or provision of criminal, operational or other compromising information.

1196. Requests were submitted by the following countries: Uzbekistan, Russia, Estonia, Latvia, Hungary, Turkey, Belarus, Kyrgyzstan, Czech Republic, Switzerland, Belgium, USA, Ireland, etc.

1197. The NSC maintains active international cooperation in both bilateral and multilateral forms. The measures were realized to create a global network for fighting international terrorism. Quite efficient measures for joint countering regional challenges were implemented on the basis of the CIS ATC and the SCO RCTS.

1198. At the same time, measures for improvement of cooperation between the SCO competent authorities for identification and suppression of terrorism financing channels were considered at the joint working group and round table held on the basis of RCTS in 2019 on the initiative of Kazakhstan and implemented by the decision of the Council of the SCP RCTS.

1199. Most of the investigative orders were related to criminal cases of terrorist and extremist crimes, illicit

trafficking in narcotic drugs, psychotropic substances, firearms and ammunition, illegal migration and crossing state borders (within the jurisdiction of the NSC and the relevant special services of foreign states). Generally, international orders are executed within one month.

Supervisory authorities

1200. The NB[45] cooperates with the central banks, supervising and regulatory authorities of other countries as well as with international and other organizations within its competence, and may confidentially exchange information constituting a trade secret at the security market, banking or insurance secrecy or other legally protected secret and required for the implementation of supervisory and regulatory functions on the basis of and in accordance with an international treaty of the Republic of Kazakhstan which allows exchange of confidential information. The above-mentioned organizations include associations of central banks, supervisory and regulatory authorities of other countries established for development of uniform standards for regulating the activities of the banking sector, securities market, and insurance market.

1201. Thus, the specified exchange of confidential information is carried out for the purposes of financial supervision on the basis of both bilateral cooperation and multilateral mechanism of cooperation by joining the relevant memorandums (agreements) of international associations of national financial regulators in the corresponding part of the financial sector, and specifically for the purposes of AML/CFT supervision.

1202. The NB concluded 43 agreements and memorandums with foreign central banks - regulators in the sphere of cooperation in exchange of confidential information / exchange of information in the financial and banking sphere, including in the AML/CFT sphere.

1203. The NB uses other forms of international cooperation to exchange information. In particular, in accordance with the decision of the Council of Heads of Central (National) Banks of the Member States of the Treaty on the Establishment of the Eurasian Economic Union, information on changes in the current legislation of the Republic of Kazakhstan on currency regulation and currency control, combating money laundering and terrorist financing is sent to the Interstate Bank on a semi-annual basis; as part of the Working Group on Currency Regulation and Currency Control of the Republic of Kazakhstan the information on changes in the current legislation on currency control, anti-money laundering, and combating financing of terrorism is also sent to the EEU members.

1204. The forms of international cooperation include the exchange of information through e-mail, official correspondence, and videoconferencing.

Case Study 2.15 NB cooperation with foreign conterparts

As part of the execution of the Agreement on cooperation between the NB and the Central Bank of the Russian Federation in the field of supervision (oversight)/monitoring of payment systems, the NB provided statistical information on money transfers in the territory of the Parties for 2019-2020, information on the volume and number of money transfers through money transfer systems from Kazakhstan to Russia and back, on the approaches to assessment conducted by the parties for compliance with the Principles for financial market infrastructures, and on legislative changes within the mechanism. Similar information was also received from the Central Bank of the Russian Federation;

Provided information of an explanatory nature in response to a request from the Federal Tax Service of the Russian Federation (2020);

A questionnaire of the Central Bank of Azerbaijan on AML/CFT work organization was filled in (2020);

Participated in an online meeting with the U.S. diplomatic mission to discuss AML/CFT issues (2021).

1205. Within the framework of the Cooperation Agreement, the NB provides for joint supervision of the payment systems, as well as the development of proposals on the mechanism of interaction between regulators in the framework of joint supervision, including also response measures when AML/CFT

[45] RK Law of the National Bank of the Republic of Kazakhstan No. 2155 dated March 30, 1995.

requirements are violated.

1206. The ARDFM maintains international cooperation on the issues of business reputation of owners and heads of financial institutions and unfair practices in the financial market, specifically in the context of exchange of information on schemes of legalization (laundering) of criminal proceeds and the financing of terrorism known to the supervisory authorities and on persons involved in implementation of such schemes. This also covers compliance of the national AML/CFT legislation by parent organizations and their cross-border organizations.

1207. Under corresponding agreements, requests, including but not limited to those on AML/CFT were submitted (Russia, Belarus, Uzbekistan, Ukraine, Georgia, China, Egypt, Moldova, and Tajikistan). Information was provided on suspicious activities of companies, on the beneficial owners of the listed companies, on the system of risk-based supervision, on fulfillment of contractual obligations, on pyramid scams, etc.

1208. In order to assess business reputation, obtain information on absence of a criminal record within the framework of the BDR, the Agency requests information from the public authorities of other countries, including but not limited to those no agreements have been concluded with. Thus, from 2017 till the first half of 2022, within the framework of the concluded agreements, the Agency sent 167 requests[46] and received 73 requests from regulators[47]. All the requests were responded.

Case Study 2.8 Background check of a foreign person

In 2018, there were 2 refusals to approve bank executives on the ground of no impeccable business reputation according to the information received from the Central Bank of the Russian Federation.

In the process of approval of Candidate 1 (a citizen of the Russian Federation) for an executive position in a resident bank in the Republic of Kazakhstan, the information provided by the Central Bank of the Russian Federation revealed that Candidate 1 operated in Bank 1 in the territory of the Russian Federation. At the same time, Candidate 1 did not specify that activity in the information provided to the authorized agency. During the working life of Candidate 1, Bank 1 did not comply with the prudential liquidity requirements of the CBRF. To improve the liquidity on the request of Bank 1, the CBRF decided to provide the Bank with a special loan to maintain its liquidity, measures were taken to increase the capital of Bank 1, and an interim administration was appointed to manage Bank 1.

Based on that information and due to the facts that confirmed the lack of professionalism and integrity, Candidate 1 was denied an approval to occupy the executive position.

In the process of approval of Candidate 2 (a citizen of the Russian Federation) for an executive position in a resident bank in the Republic of Kazakhstan, the information provided by the Central Bank of the Russian Federation revealed that Candidate 2 operated in Bank 2 in the territory of the Russian Federation. By orders of the Central Bank of the Russian Federation, a temporary administration was appointed to manage the Bank 2 in 2014, and the powers of the management bodies of the Bank were suspended.

The Central Bank of Russia also pointed out that, in accordance with the requirements established by Article 16, part 1, clause 1, paragraph 13 of Federal Law No. 395-1 On Banks and Banking Activities dated December 2, 1990 (as amended on September 30, 2013), the position of the sole executive body, their deputy, or a member of the collective executive body of a credit institution within the 12 months before the day of appointment of a temporary administration for the credit institution by the decision of the Bank of Russia and suspension of the powers of its management bodies result in the business reputation

[46] Pakistan, Russian Federation, Georgia, Armenia, Belarus, Kenya, China, Germany, England, Moldova, Ireland, Kyrgyz Republic, Ukraine, Korea, Czech Republic, Japan, Poland, India, Tajikistan, Romania, Albania, Saudi Arabia, Bosnia and Herzegovina, Turkey, Croatia, Austria, Poland, United Kingdom, Kenya, Tanzania, Uganda, Belize, USA, Cyprus, Israel, Macedonia, Turkmenistan, Hong Kong, Uzbekistan, Cambodia, UAE, Estonia, Czech Republic, Bulgaria, and Hungary.

[47] Requests were received from: Kyrgyz Republic, Ukraine, Moldova, Serbia, Russian Federation, Turkey, Mongolia, Georgia, France, Philippines, Indonesia, Croatia, Tajikistan, Latvia, India, Vietnam, Bulgaria, Japan, Korea, Poland, Armenia, Pakistan, Cyprus, Ireland, Romania, Belarus, Lithuania, Slovenia, Uzbekistan, Slovenia, Qatar, and Czech Republic.

of the corresponding person to be found unsatisfactory.

Based on the information provided by the Central Bank of the Russian Federation, Candidate 2 was denied an approval to occupy the executive position.

1209. The supervisory authorities for DNFBPs did not engage in international AML/CFT cooperation, yet there are no restrictions on its implementation when necessary, which is generally consistent with the context in which DNFBPs carry out their activities. . The supervisory authorities are also aware of the capacity of the AFM in terms of international cooperation.

1210. Assessors came to a conclusion that the level of international cooperation in the field of supervision complies with the needs of regulators and possible risks.

8.2.4. Exchange of basic information and information on beneficial owners of legal entities and arrangements

1211. According to the FMA, information for the purposes of identifying beneficial owners is requested and provided in the vast majority of requests, (see Example 2.17). According to the information provided by the country, of all FIU requests by the FIU 54% of them were related to identification of beneficial ownership.

1212. The assessors believe that there are no obstacles to the collection and provision of relevant information under MLA procedures in the country. Firstly, there is no information from foreign partners, who provided feedback in the FATF Global Network, about cases when the Republic of Kazakhstan refused to provide such information or could not provide it. Secondly, there are no prohibitions or other regulatory obstacles in the legislation of the Republic of Kazakhstan to transfer such information to foreign counterparts, and the necessary legal framework for the implementation of measures to collect such information has been established.

1213. In these circumstances, and with appropriate practice, all competent authorities are able to obtain and transmit information on beneficial owners through MLA channels.

1214. During the on-site mission, the representatives of the competent authorities demonstrated a common understanding of the algorithm of actions when dealing with relevant requests. The LEAs/SSAs successfully identified the ultimate beneficiaries in the course of criminal investigations through the MLA channels.

1215. According to the statistics for 2017-2022 provided by the GPO, out of 123 ML requests sent through MLA channels, 42 requested information on the beneficial owners of companies that were used in the legalization of criminal assets. In particular, requested information from foreign competent authorities included the registration of companies and their beneficial owners, bank files, founding documents, powers of attorney, orders and other documents of companies suspected of criminal activity. The requests were mostly sent to offshore jurisdictions (Isle of Man, Marshall Islands, British Virgin Islands, Belize, Gibraltar, Dominica, Seychelles, Saint Vincent and the Grenadines and the UAE). As a result, approximately 2,000 criminal companies have been identified and are subject to asset freezing measures.

Case Study 2.17 Use of established beneficial ownership information

Information about the beneficiaries was used by the aggrieved party in civil proceedings in the U.S. and the UK on claims to legalize criminal proceeds and freeze assets abroad.

Evidence has been shown in U.S. court, including constituent documents with the signatures of M.A., which were obtained by GPO under the MLA from the offshore Isle of Man and the UAE in 2017-2019.

This evidence was turned over to JSC "B Bank" (as an aggrieved party in the criminal case) for use in the civil litigation.

As a result, in 2022, a U.S. court granted the Bank's claims and found that M.A., I.H. and their

accomplices had laundered the Bank's stolen assets in the United States.

The jury awarded the Kazakhstan more than $200 million in damages.

Similarly, in the UK courts in the case of M.A. and I.H.'s confession to legalization of the stolen money in the Bank, the injured party presented evidence (obtained during the investigation of the criminal case) revealing the real beneficiaries.

As a result, the court issued freezing orders on more than 1,500 companies controlled by the organized criminal community of M.A. and I.H.

1216. Despite the fact that LEAs generally have qualified and well-trained specialists, the assessors recommends that systematic work be continued.

Overall conclusion on IO.2

1217. The Republic of Kazakhstan ensures the provision of MLA and extradition in a constructive and timely manner. The FATF Global Network provided mostly positive feedback. Kazakhstan, in accordance with the country risk profile, seeks official assistance in the prosecution of ML/TF and related predicate offenses that involve transnational elements. The competent authorities are confident in resorting to MLA mechanisms in the cases under investigation. Extradition is requested successfully in most cases.

1218. LEAs effectively cooperate and exchange information in other forms in various international venues. Such cooperation leads to concrete, practical results.

1219. Information exchange through the FIU is implemented on an ongoing basis with a wide range of counterparties and its nature is consistent with national ML/TF risks. Representatives of the FIU demonstrated various tools and channels of international cooperation, which can cover not only the needs of the financial intelligence itself, but also other LEAs/SSAs.

1220. The authorities of the Kazakhstan generally cooperate effectively on extradition and most of the relevant incoming requests are granted. One tenth of the refusals to extradite from the Kazakhstan are related to the legal prohibition to extradite one's own citizens. In cases where a person has absconded from law enforcement authorities, the national authorities take measures to locate and extradite him/her.

1221. International cooperation on supervisory issues is limited. Supervisory authorities for FIs are parties to international agreements and other relevant international organizations and there is no legislative barrier to the exchange of relevant information. Assessors conclude that the level of international supervisory cooperation is generally consistent with the needs of regulators and the risks at this stage.

1222. All competent authorities receive and transmit information on beneficial owners through the MLA channels and other forms of international cooperation.

1223. **The Republic of Kazakhstan is rated as having a substantial level of effectiveness for IO.2.**

ANNEX: ASSESSMENT OF TECHNICAL COMPLIANCE

Recommendation 1 – Assessing Risks and Applying a Risk-Based Approach

1224. Recommendation 1 was added to the FATF Recommendations in 2012, so compliance with this Recommendation's criteria was not analyzed during the first round of the EAG mutual evaluations.

1225. **Criterion 1.1**– In the Republic of Kazakhstan, ML/TF risk identification and assessment processes were mainly carried out as part of the national risk assessments conducted in 2018 and 2021. For the purposes of the NRA, they used own data collection methodologies (Orders of the Minister of Finance No. 196 dated March 29, 2017 and No. 80 dated January 30, 2020, as well as FMA Chairman's Order No. 291-nk dated October 1, 2021), comprehensive methodological approach to conducting the NRA based on the FATF, OSCE and World Bank guidance documents, as well as quantitative and qualitative data from various sources (statistics and analytics of law enforcement, supervisory and other government authorities, information on financial transactions reported to the FMA, results of surveying government authorities and obliged entities, open data, etc.)

1226. The 2021 NRA was conducted by the FMA (coordinator in accordance with AML/CFT Law, Article 16, Par. 13-3) in cooperation with the competent authorities and representatives of the obliged entities. For this purpose, an interagency working group was established, the composition of which was approved by the FMA Chairman's Order. Public and non-public versions of the report were prepared and approved at the meetings of the AML/CFT Interagency Council (IAC) on August 20, 2021 and October 13, 2021, respectively.

1227. Besides that, the FMA conducted separate risk assessments of the banking and insurance sectors, entities engaged in certain types of banking transactions, securities market, microfinance organizations. The FMA developed a methodology for conducting SRAs in the activity areas of the following obliged entities: lawyers, accountants and auditors, entities engaged in leasing activities without a license, DPMS sector entities, realtors.

1228. **Criterion 1.2** – The FMA, as the AML/CFT/CPF authority, coordinates the ML/TF risk assessment and implementation of mitigation measures (AML/CFT Law, Article 16, Par. 13-3). In order to strengthen cooperation, a dedicated interagency format of the IAC (formerly known as the Interagency Commission chaired by the Minister of Finance, abolished in September 2020) headed by the FMA First Deputy Chairman (AML/CFT Law, Article 11-1, Par. 3-6) was established. The IAC is composed of deputy heads of the government authorities engaged in combating ML/TF/PF. In addition to coordinating ML/TF risk assessment activities, the IAC develops government policy and opinions on international cooperation issues in the AML/CFT sphere, makes legislative proposals and implements other tasks pertaining to improving the effectiveness of the national AML/CFT system.

1229. **Criterion 1.3** – NRAs are stipulated by law and conducted once every three years (AML/CFT Law, Article 11-1, Par. 13-3, Article 16, Par. 4 of RK Government Resolution No. 243 dated May 3, 2017). The NRA lasts no longer than 18 months, the next NRA is held after 36 months from the date of the previous one (Par. 3 of the FMA Chairman's Order No. 14 dated February 23, 2022).

1230. **Criterion 1.4** – The FMA is obliged to submit the risk assessment report to the relevant government authorities and to publish information from this report on its website (AML/CFT Law, Article 11-1, Par. 5; Par. 26 of the FMA Chairman's Order No. 14 dated February 23, 2022). The NRA findings are sent to all concerned government authorities for use in their work and are disseminated to the obliged entities – both by publication on the FMA website and by sending them to personal accounts of the obliged entities on the FMA portal. The obliged entities should take into account the key NRA findings set out in the public version of the report when implementing their internal control rules (AML/CFT Law, Article 11-1, Par. 5).

1231. At the same time, there is no information about the mechanisms for communicating information from the risk assessment report to SRBs. In the opinion of the assessment team, the fact of publication on the

official website without the relevant obligation cannot be a sufficient tool to perform this task.

1232. **Criterion 1.5**– The FMA is responsible for developing measures aimed at mitigating ML/TF risks and submitting them to the Government for approval (AML/CFT Law, Article 16, Par. 13-4). Based on the 2018 NRA findings, measures aimed at mitigating ML/TF risks were approved in the Republic of Kazakhstan (RK Government Resolution No. 602 dated August 16, 2019). The above measures include supervisory, typological, methodological, regulatory, organizational and information technology actions. This resolution also sets time frames for the implementation of measures and agencies responsible for their implementation. The number of measures developed on the basis of the findings of the two 2018 ML/TF risk assessments is very limited (a total of 16 measures). Besides that, the approved measures are quite general in nature, often making it impossible to attribute them to the mitigation of any particular risk. There are no measures aimed at increasing the transparency of beneficial ownership of legal entities and the development of international cooperation mechanisms.

1233. On the basis of the 2021 NRA conclusions, RK Government Resolution No. 915 on Approval of Measures Aimed at Mitigation of Risks of Legalization (Laundering) of Criminal Proceeds and Terrorist Financing dated December 20, 2021 was adopted. Despite attempts to link the nature of measures to certain types of predicate offences, as well as the regular work of the anti-money laundering system stakeholders (development of typologies, increased international cooperation, control inspections of the obliged entities, etc.), the developed areas of work are few (26 items) and represent very general measures, often unrelated to the presence of a particular risk included in the NRA report.

1234. In order to improve control over the implementation of measures contained in the Risk Mitigation Plans, it is advisable to provide for the allocation of resources and the development of control indicators to identify factors impeding the implementation of these Plans.

1235. There is also an approach to developing risk mitigation measures at the strategic level. Thus, a number of national and sectoral policy documents (National Development Plan until 2025 adopted by RK Presidential Decree No. 636 dated February 15, 2018; National Security Strategy for 2021-2025 adopted by RK Presidential Decree dated June 17, 2021 and Action Plan for National Security Risk Management; Concept of Development of Financial Sector until 2030 adopted by RK Government Resolution No. 954 dated August 27, 2014; Anti-Corruption Strategy for 2015-2025 adopted by RK Presidential Decree No. 986 dated December 26, 2014; State Program of Combating Religious Extremism and Terrorism in the Republic of Kazakhstan for 2018-2022 adopted by RK Government Resolution No. 124 dated March 15, 2018; Comprehensive Action Plan for Suppressing Shadow Economy for 2021-2023 adopted by RK Government Resolution No. 644 dated September 21, 2021, etc.) also contain tasks and measures for neutralizing the identified risks.

1236. **Criterion 1.6**

a) There are no situations in Kazakhstan where the obliged entities are not required to comply with the FATF Recommendations.
b) The legislation provides for the non-applicability of customer due diligence measures (AML/CFT Law, Par. 3-1(1)) for FIs and DNFBPs for certain one-time transactions. The threshold amounts under these exemptions are much lower than the threshold amounts set out in the FATF Recommendations and are largely inapplicable when the obliged entities have suspicions of ML/TF.

1237. Criterion 1.7 (Met) – According to AML/CFT Law, Article 11-1, Par. 6, the obliged entities shall take into account the published NRA information when implementing programs included in the ICR, in particular: i) assess, identify, document and update ML/TF risk assessments; ii) develop ML/TF risk management and mitigation controls and procedures; and iii) classify their customers based on ML/TF risk. In accordance with AML/CFT Law, Article 5, Par. 7, enhanced CDD measures shall be applied by entities in the cases and in the manner prescribed by the internal control rules and depending on the ML/TF risk level. In accordance with the ICR Requirements, the obliged entities shall apply enhanced CDD measures to high-risk customers.

1238. Enhanced risk mitigation measures include determining the reasons for planned or conducted transactions, increasing the number and frequency of inspections and identifying the nature of transactions for in-depth examination, obtaining information on the type of activity and source of funding of transactions being conducted, obtaining senior management's approval to establish or continue business relationships with customers. Besides that, the obliged entities are required to refuse to establish business relationships with a natural or legal person and/or conduct a transaction if it is not possible to conduct customer due diligence (as required by AML/CFT Law, Article 5, Par. 3). The obliged entities also have the right to refuse to conduct customer transactions, establish business relationships and terminate business relationships with customers if there is suspicion that customers are using business relationships for ML/TF purposes.

1239. There are also additional enhanced measures for customers who are national and foreign politically exposed persons (AML/CFT Law, Article 8).

1240. **Criterion 1.8**– Pursuant to AML/CFT Law, Article 5, Par. 7, the application of simplified CDD measures includes the implementation by the obliged entities of the following steps: i) reducing the frequency of customer's identity details updates; ii) reducing the frequency of business relationships verification and customer transactions inspection; and iii) determining the purpose and nature of business relationships based on the nature of transactions. Simplified CDD measures are not applicable if the obliged entities have reasons to believe that the purpose of establishing business relationships or conducting transactions is ML/TF. The application of simplified CDD measures when identifying a low risk level of the customer is stipulated by similar provisions of the Internal Control Rules of various categories of obliged entities.

1241. Simplified CDD can only be carried out if the low risk conclusions made by the obliged entities are consistent with the findings of the national risk assessment. Besides that, simplified CDD measures do not apply if an obliged entity has reasons to believe that the purpose of business relationships or transactions is ML/TF.

1242. **Criterion 1.9**– In accordance with Article 14 of the AML/CFT Law, state control over compliance of the obliged entities with legislation in terms of recording information, keeping information and documents, protection of documents, providing information on transactions with funds and/or other assets that are subject to financial monitoring, carrying out due diligence of customers (their representatives) and beneficial owners, taking measures to freeze transactions with funds and/or other assets, suspending and rejecting transactions that are subject to financial monitoring, as well as developing and implementing a system of checks and balances, and developing and approving the internal control rules, including the execution of the training and education program, shall be carried out by the relevant government authorities in accordance with their purview and in the manner prescribed by the legislation of the Republic of Kazakhstan. According to AML/CFT Law, Article 11(2), Par. 3-4, the ICR requirements for AML/CFT purposes by type of obliged entity are established by the relevant government authorities.

1243. The procedure for state control and supervision is established by the RK Commercial Code (Article 138, Subpar. 57), which stipulates controlled activity areas of business entities, and detection and prevention of ML/TF offences is reflected in the checklist approved jointly with the authorized body and the regulatory government authorities (RK COMC, Article 85).

1244. Besides that, CAO Article 214 provides for sanctions that can be imposed on the obliged entities for failing to comply with their obligations to develop and adopt the ICR and implementation programs or if the ICR fail to meet legal requirements. The AML/CFT Law requires the obliged entities to assess and manage the risks to which they are exposed as part of their internal control systems (see criteria 1.10 and 1.11). For additional information on the essential elements and deficiencies of the control and supervisory regime, see criteria 26.1, 26.4, 28.2 and 28.5.

1245. **Criterion 1.10**

a) The requirement for the obliged entities to assess, identify, document and update ML/TF risk assessment findings is set out in AML/CFT Law, Article 11-1, Par. 6(1). Besides that, similar provisions for individual obliged entities are contained in the ICR requirements for individual categories of the obliged entities.

b) The ICR requirements for most categories of the obliged entities require consideration of all relevant risk factors before determining the overall risk level. This includes risk by customer type, country (geographic) risk, service (product) risk and/or the manner in which it is provided.

It is also envisaged that the assessment of the degree of exposure of the entity's services (products) to ML/TF risks is accompanied by a description of possible measures aimed at mitigating the identified risks, including changes in procedures for identifying and monitoring customer transactions, setting transaction thresholds, changing the terms of services (products) provision, refusal to provide services (products).

c) The obligation of the obliged entities to keep risk assessments up to date is set out in AML/CFT Law, Article 11-1, Par. 6(1), as well as in the ICR requirements for various categories of the obliged entities.

These regulatory legal acts stipulate the obligation of the obliged entities to assess the degree of exposure of their services to ML/TF risks on an annual basis taking into account the ML/TF risk report information and at least the following specific risk categories: risk by customer type, country (geographic) risk, risk of service (product) and (or) the method of its (its) provision. At the same time, this issue is not covered in the regulations for the Single Pension Savings Fund and Voluntary Pension Savings Funds.

d) The ICR requirements for the obliged entities include obligations to provide risk assessment information to the relevant government authorities.

1246. **Criterion 1.11**

a) According to AML/CFT Law, Article 11, Par. 3, the obliged entities are required to develop the ICR and programs to implement them. In addition to requirements to the activities of the obliged entities when excersizing the internal control, the ICR must include a number of programs, including an ML/TF risk management program that addresses customer risk and the risk of using services for criminal purposes, including the risk of using technological advances.

According to AML/CFT Law, Article 11-1, Par. 6 and ICR Requirements for various categories of the obliged entities (other than commodities exchanges), the published NRA report information shall be considered in implementing a risk management program.

In accordance with the ICR Requirements for certain categories of the obliged entities (insurance organizations, insurance brokers, STBs and the National Postal Operator, stock exchange, entities engaged in certain types of banking transactions, except for the operator or operating center of the interbank money transfer system and microfinance organizations, professional securities market participants and central depository, SPSF and VPSF), the ICR are developed and adopted by the managing or executive bodies of the obliged entities (AML/CFT Law, Article 11, Par. 3) and are an internal document of the obliged entities or a set of such documents. However, the regulations governing the ICR Requirements for other categories of the obliged entities do not explicitly state that the ICR shall be approved by the obliged entities' senior management.

b) The regulatory legal acts governing the ICR Requirements for various categories of the obliged entities contain provisions that the internal control program shall include procedures for preparing and providing senior management with the managerial accounting records on the findings of an assessment of the internal control effectiveness for AML/CFT purposes.

There are also provisions that the responsible officer and AML/CFT unit officers shall prepare information on the implementation of the internal control rules and recommended measures to

improve ML/TF risk management and internal control systems for AML/CFT purposes and report to senior management.

c) See also Criterion 1.7. Pursuant to Article 11-1(6) of the AML/CFT Law, the obliged entities shall consider the published NRA information when implementing the ICR, in particular developing control measures and ML/TF risk management and mitigation procedures. Depending on the customer risk level, the extent of measures taken by the obliged entities is expressed in the application of simplified or enhanced customer due diligence measures. This requirement is also contained in a number of regulatory legal acts, defining the ICR Requirements for different categories of the obliged entities.

There are are no provisions on application of these measures in the ICR Requirements for the Single Pension Savings Fund and Voluntary Pension Savings Funds.

1247. **Criterion 1.12**– Provisions on the application of simplified risk-based measures are reflected in the obliged entities' regulations, defining the ICR requirements (see Criterion 1.11). Also, pursuant to AML/CFT Law, Article 5, Par. 7, simplified CDD measures do not apply if the obliged entities have reasons to believe that the purpose of business relationships or customer transactions is ML/TF. According to AML/CFT Law, Article 5, Par. 7, simplified CDD measures are applied to customers (their representatives) and beneficial owners at low ML/TF risk assigned by the obliged entities in accordance with the risk management program provided for in the ICR.

Weighting and conclusion

1248. The Republic of Kazakhstan has made significant efforts to ensure technical compliance with Recommendation 1. The main deficiencies are associated with the need to refine approaches to the identification and assessment of TF and PF risks, as well as in the obliged entities sectors, develop mechanisms for disseminating the risk assessment report information to SRBs, FIs and DNFBPs, build a comprehensive risk-based approach to implementing risk mitigation measures, as well as synchronize the exemptions from customer identification obligations with the findings of specific national or sectoral risk assessments.

1249. **Recommendation 1 is rated largely compliant**

Recommendation 2 – National Cooperation and Coordination

1250. In the 2010 mutual evaluation report, the Republic of Kazakhstan was rated "PC" with Recommendation 31. The assigned rating was due to deficiencies related to the fact that the assessors were not provided with materials on bilateral mechanisms of operational interaction and feedback among the FMC, law enforcement and supervisory authorities. In this regard, at the time of the first round of mutual evaluations in the Republic of Kazakhstan, the FIU, law enforcement, supervisory and other competent authorities did not have effective mechanisms in place that would allow them to cooperate with each other internally to develop and implement AML/CFT policies and activities.

1251. **Criterion 2.1**– In the following documents defining the strategic directions of state policy, the AML/CFT issues (including the application of risk-based supervision in this area) are identified as priorities: National Development Plan[48], National Security Strategy and Action Plan[49], Concept of Legal Policy[50], Concept of Development of Financial Sector[51], Anti-Corruption Strategy[52], State Program on Combating Religious Extremism and Terrorism[53], Agreement between the Government, National Bank and

[48] National Development Plan until 2025 adopted by RK Presidential Decree No. 636 dated February 15, 2018
[49] National Security Strategy of the Republic of Kazakhstan adopted by RK Presidential Decree dated June 17, 2021 and Action Plan for National Security Risk Management
[50] Concept of Legal Policy until 2030 adopted by RK Presidential Decree dated October 15, 2021
[51] Concept of Development of Financial Sector of the Republic of Kazakhstan until 2030 adopted by RK Government Resolution No. 954 dated August 27, 2014
[52] Anti-Corruption Strategy of the Republic of Kazakhstan for 2015-2025 adopted by RK Presidential Decree No. 986 dated December 26, 2014
[53] State Program of Combating Religious Extremism and Terrorism in the Republic of Kazakhstan for 2018-2022 adopted by RK Government Resolution No.

Agency for Regulation and Development of Financial Market of the Republic of Kazakhstan[54], Comprehensive Action Plan on Supressing Shadow Economy[55], Interstate Program of Joint Measures to Combat Crime[56], Action Plan of the Government of the Republic of Kazakhstan for Combating Human Trafficking-Related Crimes[57].

1252. **Criterion 2.2**– According to AML/CFT Law, Article 15, Subpar. 1, one of the FMA's tasks is to implement a unified AML/CFT state policy. One of the functions of the FMA is to coordinate the AML/CFT activities of government authorities (AML/CFT Law, Article 16(1), Subpar. 3). Besides that, according to AML/CFT Law, Article 11-1, Par. 3, in order to develop measures to implement government AML/CFT policies, improve their effectiveness, as well as to coordinate ML/TF risk mitigation measures, the IAC was established through which the FMA performs its coordinating functions.

1253. **Criterion 2.3**– The main tasks of the IAC are to develop measures to implement AML/CFT state policy, to increase their effectiveness, as well as to coordinate ML/TF risk mitigation measures (AML/CFT Law, Article 11-1, Par. 3). The Interagency Council is composed of representatives of law enforcement and special government authorities of the Republic of Kazakhstan, as well as government authorities engaged in AML/CFT activities in accordance with the AML/CFT Law.

1254. Another mechanism for coordinating the activities of law enforcement, supervisory and other government authorities and organizations is the Interagency Working Group under the auspices of the Presidential Executive Office for preparing the Republic of Kazakhstan for the second round of the EAG mutual evaluations (hereinafter the IAWG, established by Order of the Head of the Presidential Executive Office No. 21-01-38.29 dated July 29, 2021). The IAWG is composed of representatives of all key government authorities participating in the national AML/CFT system. In addition to preparing for mutual evaluations, the main tasks of the IAWG also include the implementation of measures generally aimed at increasing the level of technical compliance with the FATF Recommendations and the effectiveness of the AML/CFT/CPF system, monitoring law enforcement practices and interagency coordination in combating illegal financial transactions and suppressing the operation of shadow schemes in the financial market.

1255. Interagency formats have been created and are functioning on certain topical issues. In accordance with the Prime Minister's order, a Working Group was established to implement a pilot project on crypto exchanges' activities in the AFSA (approved by Order of the MDD No. 207/NK dated June 11, 2021). Besides that, the Interagency Working Group for elaboration of measures aimed at suppressing pyramid schemes composed of the ARDFM, NB, GPO, FMA, MISD and MIA was established (by the ARDFM Chairman's Order No. 388 dated October 7, 2020). An Interagency Working Group was established to develop, review and approve a draft Action Plan for Suppressing Non-Observed (Shadow) Economy and ML/TF Risk Mitigation for 2021-2025 composed of the competent government authorities, organizations and associations. Interaction of the GPO with law enforcement authorities is carried out within the framework of the Law Enforcement and Anti-Crime Coordinating Council.

1256. Mechanisms of operational interagency cooperation in the AML/CFT sphere between the FMA and other competent authorities are also being developed. In particular, by joint orders with the MoH, APDC, MCS, MoF and MoJ, Action Plans for the obliged entities' compliance with the AML/CFT Law provisions were approved, which contain a number of measures for implementing joint awareness-raising activities on the issues of the obliged entities' compliance with the AML/CFT legislation, applying risk assessment criteria, identifying and analyzing risks, developing risk mitigation measures, as well as risk assessment recommendations and instructions.

---

124 dated March 15, 2018

[54] Agreement between the Government, National Bank and Agency for Regulation and Development of Financial Market of the Republic of Kazakhstan on Coordination of Macroeconomic Policy for 2021 – 2023 adopted by RK Government Resolution No. 90 dated February 23, 2021

[55] Comprehensive Action Plan for Suppressing Shadow Economy for 2021-2023 adopted by RK Government Resolution No. 644 dated September 21, 2021, formerly known as Action Plan for Suppressing Shadow Economy for 2019-2021 adopted by RK Government Resolution No. 921 dated December 29, 2018

[56] Interstate Program of Joint Measures to Combat Crime for 2019-2023 adopted by the Resolution of the Council of Heads of the CIS Member States on the Interstate Program of Joint Measures to Combat Crime for 2019-2023 dated September 28, 2018

[57] Action Plan of the Government of the Republic of Kazakhstan for Combating Human Trafficking-Related Crimes for 2021-2023 adopted by RK Government Resolution No. 94 dated February 24, 2021

1257. The FMA has concluded agreements with all the competent authorities on cooperation and information exchange. In particular, the Agreement with the MoF (joint order of the FMA Chairman and the Minister of Finance No. 68-nk dated April 21, 2021), AML/CFT cooperation and collaboration agreements between the FMA and MISD (dated March 16, 2021), between the FMA, NB and ARDFM (dated March 31, 2021), as well as between the MoF, NB and FMA (No. 72 dated July 30, 2020), under which, *inter alia*, AML/CFT information exchange, as well as analytical information and statistical data provision, are carried out. A Memorandum of Cooperation and AML/CFT Information Exchange was concluded between the AFSA and the FMA.

1258. **Criterion 2.4** – The authority to counter the financing of proliferation of weapons of mass destruction is vested in the FMA (AML/CFT Law, Article 1(1), Subpar. 13). The procedure for interaction beyween the FMA and the government, law enforcement and special government authorities is determined by Order 1009/dsp and Order 274. Besides that, the CPF issues are included in the authority of the MIA (FMA Chairman's Order No. 251-nk dated September 03, 2021).

1259. **Criterion 2.5** – In accordance with the Law 94-V, personal data in the Republic of Kazakhstan is divided into public and confidential (Article 6). It also provides for the procedure for dealing with personal data obtained with the person's consent (Articles 7 and 8 of the above law), as well as the cases when the collection and processing of personal data is possible without the person's consent (Article 9 of the above law). Besides that, AML/CFT information exchange can be carried out within the frame of interagency agreements concluded by the FMA with all the Kazakh competent government authorities.

1260. At the same time, according to the AML/CFT Law, government authorities shall ensure appropriate storage, protection and integrity of information, records and documents constituting official, commercial, banking or other legally protected secrets obtained in the course of their activities (AML/CFT Law, Article 18, Par. 1(3) and Article 18, Par. 2(4)).

1261. **Recommendation 2 is rated compliant.**

Recommendation 3 – Money laundering offence

1262. In the 2011 Mutual Evaluation Report, the country was rated "Partially Compliant" with regard to the criminalization of the ML offence. The main deficiencies noted by the experts were: (i) inconsistency of the disposition of the CC Article, which establishes liability for ML, with the provisions of the Vienna and Palermo Conventions (no criminalization of ML in the forms of conversion and transfer of property; concealment or disguise of the true nature, source, location, method of disposal, movement, rights to property or its ownership); possession or use of the criminal property for personal purposes; (ii) ML does not extend to property that is the indirect proceeds of crime; (iii) insider dealing and market manipulation are not criminalized; (iv) TF is not a predicate offence for ML; (v) there is no administrative or criminal liability of legal persons under the national law.

1263. After the previous mutual evaluation, the Republic of Kazakhstan adopted a new CC (Law No. 226-V dated July 3, 2014) and the CAO (Law No. 231-V dated July 4 2014).

1264. **Criterion 3.1 -**The UN Conventions Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and Against Transnational Organized Crime (Palermo Convention) were ratified without reservations (Laws No. 246 dated June 29, 1998, and No. 40-iv dated June 4, 2008).

1265. Criminal liability for ML is established by CC Article 218 Legalization (Laundering) of money and/or other property obtained by criminal means. Based on the disposition of the above norm, as well as clarifications contained in Par. 19 of SC Resolution No. 3 dated January 24, 2020[58], legalization is the disposal of money or other property obtained through the commission of a criminal offence in the following forms: (i) introduction into the legal circulation through transactions in the form of conversion or transfer

[58] Regulatory resolutions of the Supreme Court of the Republic of Kazakhstan are acts of judicial interpretation containing clarifications on issues of implementation in judicial practice of the Constitution, laws, regulations, international treaties of the Republic of Kazakhstan; are regulatory legal acts being an inseparable part of the RK legislation (CC Article 1(2)) and are generally binding.

of property representing proceeds of criminal offences; (ii) possession and use of such property; (iii) concealment or disguise of its true nature, source, location, disposition, movement, rights to property or its ownership. Intermediation in legalization is equal to the ML offence and the liability for this act also comes under CC Article 218.

1266. The mandatory element of the subjective aspect of the ML offence is the special purpose of financial transactions and other deals with the property obtained by criminal means – giving a legitimate appearance to the possession, use and disposal of such property. Disposition of the above property by the guilty person in the absence of a special purpose does not form the elements of the ML offence (Par. 19 of SC Resolution No. 3 dated January 24, 2020). Criminal liability for the acquisition, possession or use of the property known to be obtained by criminal means (in the absence of a special purpose of legalization) is stipulated by CC Article 196.

1267. **Criterion 3.2. –**The country considers any criminal offence under special part of the CC to be a predicate offence for money laundering if criminal proceeds are generated as a result of it. The Criminal Law criminalizes all categories of offences designated by the FATF Recommendations.

1268. According to CC Article 31(5), participants of organized criminal groups are criminally liable for the totality of the crimes committed – for participation in such groups (CC Articles 262-265, 268) and for specific offences in the preparation or commission of which they participated. At the same time, according to the CC, the commission of a number of predicate offences by a criminal group is considered as a qualifying factor and entails stricter criminal liability.

1269. **Criterion 3.3. –**According to the disposition of CC Article 218, the legalization of proceeds of any criminal offence in any amount constitutes the ML offence. Therefore, the threshold approach is not used to define predicate offences in the country.

1270. **Criterion 3.4. –**The subject of the ML offence is "funds and/or other property obtained by criminal means". The CC and the AML/CFT Law do not define these concepts. According to Article 115 of the RK Civil Code, the property includes: items of property, money, including foreign currency, financial instruments, works, services, objectified results of creative intellectual activity, trade names, trademarks and other means of products identification, property rights, digital assets and other property. According to Article 117 of the RK Civil Code, the property is divided into immovable (land plots, buildings, facilities, perennial plantations, and other property) and movable (money, securities, and other property). Subsoil, waters, flora and fauna, and other natural resources are classified as state property; other property, including land and strategic facilities, may be in private ownership (RK Civil Code, Articles 191-193-1).

1271. The ML offence applies to any type of property directly obtained by criminal means, regardless of its value. Large-scale money laundering (in an amount exceeding 20 thousand monthly calculation indices (MCI)[59], which is approximately USD 128 thousand) entails stricter criminal liability (CC Article 218(3)).

1272. Law No. 131-VII amended the disposition of CC Article 218, according to which any proceeds derived from property obtained by criminal means were also included in the subject of legalization. Thus, indirect proceeds of crime (profit or benefit derived from the use of criminal property) are the subject of money laundering and legalization of indirect proceeds is criminalized.

1273. **Criterion 3.5. –**According to CPC Article 113(3), circumstances proving that property was illegally obtained, including through a criminal offence, and that it is the proceeds derived from the criminal property, shall be proven in a criminal case. According to CPC Article 111, evidence in a criminal case is legally obtained factual data (testimony of trial participants, conclusions of an expert, specialist, physical evidence, records of procedural and other actions), on the basis of which the presence or absence of an act stipulated by the CC and other circumstances relevant to the proper adjudication of a case are established in the manner prescribed by law. Therefore, in proving that the property is the proceeds of a crime, a

[59] Monthly Calculation Index (MCI) is a coefficient for calculating benefits, other social payments, as well as for applying penalties, taxes and other payments established by the law on the budget for the relevant year. The MCI for 2016 (in KZT) was 2,121, for 2017 – 2,262, for 2018 – 2,405, for 2019 – 2,525, for 2020 – 2,778, for 2021 – 2,917, for 2022 – 3,063. (www.egov.kz).

mandatory prior conviction of the person for the predicate offence is not required. However, for the purposes of criminal liability for ML, it must necessarily be established that the legalized property was derived from the commission of a criminal offence, which follows directly from the disposition of CC Article 218.

1274. **Criterion 3.6. –**Citizens of Kazakhstan, as well as foreign citizens and stateless persons residing in the territory of Kazakhstan, in cases where they cannot be extradited to a foreign country for prosecution, shall be criminally liable under the CC for crimes committed in the territory of another country under the following conditions: (i) the act is criminally punishable in Kazakhstan; (ii) the act is criminally punishable in the country where it was committed; (iii) the person is not convicted for this act in another country (CC Article 8).

1275. **Criterion 3.7. –**Persons who have committed the predicate offence and then the ML offence are criminally liable for the totality of the crimes committed (CC Article 13), that is, for both the predicate offence and the ML offence, in accordance with the principles of national law.

1276. **Criterion 3.8. –**Based on the provisions of CC Article 20, Par. 19 of SC Resolution No. 3 dated January 24, 2020, the ML offence belongs to the category of intentional criminal offences and the mandatory element of its subjective aspect is the offenders' awareness of the fact that a financial transaction or other deal with their participation, entrepreneurial or other economic activity are carried out with funds or other property acquired by criminal means, as well as the desire to commit such actions.

1277. According to the provisions of CPC, Articles 113, 111, the determination of the form of guilt, that is the presence of intent, is part of the fact to be proven in a criminal case, and is based on objective factual data.

1278. **Criterion 3.9. –**According to CC Article 218(1) (as amended by Law 131-VII), the following alternative punishments can be imposed for the ML offence: a fine or correctional labor of up to 5 thousand MCI (223pprox.. USD 32 thousand[60]), restriction or deprivation of freedom for a term of up to 6 years.

1279. ML committed: (i) by a group of persons by prior conspiracy[61], (ii) repeatedly, (iii) by a person exercising the powers vested in him by virtue of his office – shall be punishable by a fine or correctional labor of 3 thousand to 7 thousand MCI (USD 19.2 to 44.8 thousand), imprisonment for a term of 3 to 7 years (CC Article 218(2)).

1280. According to CC Article 218(3), criminal liability arises when ML is committed: (i) by a person authorized to perform public functions or by a person of equivalent status, an official, a person holding an important public office, if the crime is committed with the use of such persons' official powers, (ii) by a criminal group[62], (iii) in large amounts.

1281. The punishment under CC Article 218(3) has no alternative – imprisonment for a term of 5 to 10 years. For the persons who committed ML with the use of official powers, an additional punishment in the form of life-time deprivation of the right to hold certain positions or engage in certain activities is also applied. As an additional punishment, confiscation of property is stipulated by CC Article 218(1-3).

1282. On the basis of the maximum statutory term of imprisonment, the offences under Article 218 are categorized as serious crimes (prior to the amendments to Law 131-VII, the offences under CC Article 218(1,2) were categorized as crimes of medium gravity).

1283. The Criminal Law contains a number of provisions that stipulate the exemption of the person guilty of money laundering from criminal liability, the actual serving of the sentence, as well as a significant limitation of the maximum term of the sentence. According to the note to CC Article 218, the person, who voluntarily declared about the prepared or committed legalization, is exempted from criminal liability, if

[60] at the USD rate as of July 26, 2022.
[61] two or more offenders who agreed beforehand to jointly commit a criminal offence participated in the ML commission (CC Article 31(2)).
[62] a criminal group means an organized group, a criminal organization, a criminal community (including transnational), a terrorist and extremist group, a gang and an illegal paramilitary formation (CC Article 31(3)).

his/her actions do not contain elements of ML stipulated by CC Article 218(2,3) or other offences. A person who has committed the ML offence may also be exempted from criminal liability if the conditions of a procedural agreement are met (CC Article 67). In the presence of mitigating circumstances (for example, compensation for property damage, sincere repentance, incrimination of accomplices, etc.) and the absence of aggravating circumstances the punishment under CC Article 218 may not exceed two thirds of the primary punishment term or amount (CC Article 55). By virtue of the CC Article 63 provisions, the court, having imposed a sentence of imprisonment for the ML offence, may decide to consider it conditional (except for ML committed by a criminal group), which entails replacing the serving of the sentence with probationary supervision. Thus, criminal responsibility for ML is differentiated depending on the circumstances of the offence.

1284. The experts took into account the fact that the provisions of the law stipulating the possibility of exemption from criminal liability for ML or a significant limitation of the maximum term or amount of punishment are generally aimed at encouraging positive post-criminal behavior of a person.

1285. Taking into account the adjustment of CC Article 218 by Law 131-VII, the sanctions for ML are proportionate and dissuasive.

1286. **Criterion 3.10. –**The fault-based individual responsibility principle is a fundamental principle of the national legislation, in connection with which criminal liability of legal persons is not provided for in the RK.

1287. Administrative liability of legal persons is provided for, and an administrative offence means an unlawful act or inaction of a legal person (CAO Article 25).

1288. The administrative responsibility of legal persons is established for committing a transaction with funds or other assets obtained by criminal means that resulted in the legalization of such property. The period of liability for this offence is 3 years from the date of its commission. The action shall entail a fine of: MCI 750 (~USD 4.8 thousand) for small businesses; MCI 1 thousand (~USD 6.4 thousand) for medium businesses; MCI 2 thousand (~USD 12.8 thousand) for large businesses.

1289. Therefore, the fine for ML is set at the maximum amount of the fine for legal persons stipulated by the General Part of the CAO (CAO Article 44(2)). Taking into account the small amount of the fine for legal persons in monetary terms, the sanctions for ML are not fully proportionate and dissuasive.

1290. Bringing a legal person to administrative liability is not an obstacle for bringing a natural person to criminal liability. According to Article 49 of the RK Civil Code, a legal entity may be liquidated by the court decision in cases of gross violation of the law, which includes activities prohibited by legislative acts. Liquidation of legal entities in civil proceedings does not prevent a natural person from being held criminally liable.

1291. **Criterion 3.11. –**In accordance with CC Article 28, in addition to the perpetrators of ML offences, the following are considered accomplices: (i) organizer (a person who organized or directed the commission of ML offence); (ii) instigator (a person who induced another person to commit ML offence by any means); (iii) accomplice (a person who has assisted in the commission of ML offence by providing information and instrumentalities of crime, who has promised beforehand to conceal the offence). Liability of organizers, instigators and accomplices comes under CC Article 218 with reference to CC Article 28 for qualification purposes.

1292. Uncompleted forms of an offence are attempted offences (guilty actions directly aimed at committing an offence) and preparation for an offence (seeking, making or adjusting instrumentalities of crime, seeking accomplices to an offence, entering into a criminal conspiracy, etc.).

1293. Criminal liability for the preparation and attempted commission of ML offence comes under CC Article 218 with reference to CC Article 24 for qualification and sentencing purposes. At the same time, the term or amount of punishment for the ML preparation may not exceed half of the maximum term or amount of the primary punishment provided for under the relevant part of Article 218, and for the attempt

– not more than three quarters of such term or amount.

Weighting and Conclusion

1294. The ML offence is criminalized under the provisions of the Vienna and Palermo Conventions.

1295. The sanctions against legal persons for ML classified as an administrative delict are not fully proportionate and dissuasive.

1296. **Recommendation 3 is rated Largely Compliant.**

Recommendation 4 – Confiscation and provisional measures

1297. According to the outcomes of the first round of mutual evaluation, the Republic of Kazakhstan was rated "LC" with the former Recommendation 3. As deficiencies, the experts noted gaps in legal regulation in terms of confiscation of indirect proceeds of crime, confiscation of property in the possession or ownership of third parties, monetary equivalent, as well as protection of the rights of bona fide third parties.

1298. **Criterion 4.1. –**In accordance with the law, confiscation means the gratuitous removal of property from the owner by a court as a sanction for an administrative or criminal offence (Article 254 of the RK Civil Code). The CC provides for confiscation of property as an additional punishment, which is imposed by the court under conviction along with the primary punishment. According to Article 48, confiscation means the compulsory, uncompensated seizure and transfer to the state ownership of property owned by a convicted person, obtained by criminal means or acquired with criminally obtained funds, as well as property that was an instrumentality of a crime.

a) Confiscation of legalized (laundered) property: Property obtained through the commission of a criminal offence, according to CC Article 48(2), Par. 1, is subject to confiscation, which is established as an additional punishment for ML offences.

b) Proceeds of (including proceeds or other profits derived from such proceeds) or funds used or intended to be used for ML or predicate offences: in addition to confiscation of the direct proceeds of crime, any proceeds of property derived from crime are also subject to confiscation (excluding property and proceeds thereof to be returned to the rightful owner), as well as money and other property into which the property derived from the criminal offence and the proceeds thereof are partially or fully converted or transformed (CC Article 48(2), Par. 2); instrumentalities of crime (CC Article 48(2), Par. 3).

c) According to CC Article 48(2), Par. 3, money and other property used or intended for the financing or other support of extremist or terrorist activities or a criminal group are subject to confiscation.

d) Property of equivalent value: according to CC Article 48(3), if confiscation is not possible due to the use of the subject of confiscation, sale or other reason, the court shall recover from the offender a sum of money equivalent to the value of the subject of confiscation.

1299. CC Article 48 establishes legal restrictions regarding the confiscation of property. According to CC Article 48(5), the property required by a convict or his dependents according to the list established by the PEC (for example, the only housing of the convict and his family, second-hand household items, utensils, clothing, etc.), as well as money or property legalized under the RK Law on Amnesty of the RK Citizens in connection with Legalization of Property, shall not be subject to confiscation in cases where it was obtained through a criminal offence, for which the same law provides for exemption from criminal liability.

1300. In accordance with clarifications contained in Par. 20 of SC Resolution No. 4 dated June 25, 2015, if the criminal origin of the property not subject to confiscation under CC Article 48(5) is established, its monetary value shall be confiscated to the state. On the basis of these provisions, the experts concluded that the legislative limitations on the application of confiscation are not excessive.

1301. By virtue of the provisions of CC Article 48(2), Par. 1, both money and property in the possession of

the convicted person and those transferred by him to other persons are subject to confiscation.

1302. The legislation also provides for the confiscation of the illegally obtained property prior to conviction (pre-trial (non-conviction-based) proceedings for the confiscation of property). In accordance with Article 667 of the CPC, in cases where a suspect or accused person is internationally wanted or where criminal proceedings against them have been terminated on non-exonerating grounds (due to an act of amnesty, expiration of the statute of limitations for criminal liability, death), the person who conducts the pre-trial investigation initiates confiscation proceedings if there is information about the property obtained by criminal means. During the pre-trial proceedings on confiscation, the circumstances for its application shall be proved. The prosecutor files a request for confiscation to the court, and the procedural decision to approve or dismiss the request shall be made by the court.

1303. **Criterion 4.2 –**

a) The RK legislation provides norms empowering the competent authorities to identify, trace and evaluate property subject to confiscation.

   According to Article 2 of the Law 154-XIII, the tasks of agencies engaged in police intelligence activities include the detection, prevention and suppression of crimes, persons who have committed criminal offences, as well as items and documents of significance in a criminal case.

   Prior to the initiation of criminal proceedings, the identification and tracing of property subject to confiscation may be conducted in the course of the CIDA, such as interviews, inquiries, obtaining samples, operational purchase, controlled delivery, surveillance, body searches of detainees, seizure of items and documents in their possession, a search of residential premises and other sites, vehicle searches and others.

   According to CPC Article 113, the fact to be proven in a criminal case includes the existence of grounds for confiscation established by criminal law; therefore, the identification of property subject to confiscation is the responsibility of the pre-trial investigative authorities.

   In an initiated criminal case, the detection of such property may be carried out through overt investigative actions, e.g. inspection of the area, premises, items, documents (CPC Article 219), search and personal search (CPC Articles 252, 255), seizure (CPC Article 252) and covert investigative actions – site entering and (or) inspection, test purchase, etc. (CPC Article 231).

   If instrumentalities of crime, objects of crime (objects of criminal infringement), money, valuables, or other property obtained through a criminal offence are found during the inspection of the place of incident, location or premises, and if they are removed during a search, seizure or other investigative actions, such items shall be recognized as material evidence by the pre-trial investigative authority.

   In accordance with Law 2444, information about the existence and numbers of the customer's bank accounts, the balances and the movement of money in these accounts can be obtained by government authorities and officials performing the criminal proceeding functions in their criminal cases on the basis of a written request authorized by the prosecutor; by the courts in their criminal cases on the basis of a respective procedural court decision; by the prosecutor on the basis of the order to conduct inspection of the materials under review.

   Besides that, LEAs have the right to obtain information essential in conducting covert investigative activities and CIDA, as well as performing other tasks assigned to them, using the Law Enforcement and Special Authorities Information Exchange System according to the rules and on the grounds established by a joint order of the General Prosecutor, Minister of Internal Affairs, Minister of Finance, Minister for the Civil Service (for more details, see R.31).

   The rules of seizure, accounting, storage, transfer and destruction of physical evidence, seized documents, national and foreign currency, narcotics, and psychotropic substances in criminal cases by the court and procuracy, pre-trial investigative and forensic examination authorities are regulated

by RK Government Resolution No. 1291 dated December 9, 2014, but this regulatory legal act contains no provisions regarding the valuation of items recognized as physical evidence.

Pursuant to CC Article 163, the seizure of property subject to confiscation is carried out on the basis of a request by the person conducting the pre-trial investigation through a judge's decision to authorize the seizure. This procedural decision is executed by a bailiff. According to CPC Article 163(9), a specialist who determines the property value may participate in the seizure of the property. The CPC does not contain any other provisions regarding the valuation of the property at the pre-trial stage of the proceedings.

Therefore, the procedure for the valuation of the property at the pre-trial stage is not regulated in detail by the legislation.

b) Provisional measures: In order to ensure the execution of a sentence in terms of possible confiscation of property, the person conducting the pre-trial investigation is obliged to take measures to seize the property (CPC Article 161).

The procedure for taking a procedural decision on the seizure of property is given in Par. A) of this Criterion.

According to CC Article 161(7), property that is not subject to confiscation, as well as money in bank accounts and electronic money, the purpose of which is to meet various social needs (social and health insurance, improvement of living conditions, etc.) cannot be seized.

The law has a directly applicable provision allowing for the seizure of property held by other persons if there are sufficient grounds to believe that it was obtained as a result of criminal acts of the suspect or accused or used or intended to be used as an instrumentality of criminal offence or to finance extremism, terrorism or criminal groups (CPC Article 161(8)).

Besides that, CPC Article 163(4) stipulates that if there is reliable evidence that property has been obtained by criminal means and if it is not possible to identify the property, the judge has the right to seize the property of equivalent value.

The criminal procedure law does not provide for prior notification of the owner about the decision of the person conducting the pre-trial investigation to file a request for the seizure of property and the judge's consideration of the request.

The AML/CFT law also provides for the freezing of transactions with money and/or other property, which is understood to mean the suspension of the transfer, conversion, disposition or movement of money or other property. The freezing (suspension of transactions with money or other property) may be applied for criminal prosecution for ML/TF. However, this procedure does not apply to criminal cases of predicate offences (except TF).

c) Prevention of the possibility of non-application of provisional measures:

The criminal procedure law (CPC Article 161(1)) provides for the possibility of establishing a temporary restriction on the disposal of property at the pre-trial investigation stage. Such restriction is implemented by the pre-trial investigative authorities in urgent cases before filing to the court a request for the seizure of property upon the prosecutor's consent for a period not exceeding 10 days with notification within 24 hours to the property owner. The owner is not notified in the following cases: i) if the owner is not identified; ii) in criminal cases of terrorist or extremist offences; iii) in criminal cases of offences committed by a criminal group; iv) if informing the owner creates a threat of disclosure of information on covert investigative measures being conducted in the case.

Besides that, in cases where there are reasons to believe that property subject to seizure may be concealed or lost, the person conducting the pre-trial investigation may suspend transactions and other deals with the property or seize it for a period not exceeding 10 days and notify the prosecutor and the court within 24 hours (CPC Article 161(9)).

Items recognized as evidence in a case may be added to the case file or deposited for safekeeping, intended use or sale (perishable items) to other persons or institutions (CPC Article 221).

Seized property may be removed and deposited with persons and organizations that are responsible for its safekeeping (CPC Article 163).

Unlawful acts against property subject to seizure or confiscation are punishable under CC Article 425.

d) Application of appropriate investigative measures: Pre-trial investigative authorities are empowered to apply the full range of measures stipulated by the criminal procedure law, including the implementation of investigative and other procedural actions.

Procedures for temporarily restricting the disposal of property, seizure of property and the final procedural decision on confiscation are regulated in detail by the criminal procedure law.

1304. **Criterion 4.3 –**The legislation contains directly applicable norms providing for the possibility of seizure and confiscation of property owned by persons who are not suspects, accused or financially responsible for their actions (CC Article 48(2), CPC Article 161(8)).

1305. At the same time, by virtue of the provisions of Article 78 of the PEC, property transferred by a convicted person to another person is subject to confiscation if such person knew of its criminal origin. Instrumentalities of crime owned legally by a person who was not aware of the illegal purpose of their use cannot be confiscated either and shall be returned to the legal owner (CPC Article 118(3), Par. 1-1).

1306. Pursuant to CPC Article 285, when a criminal property is seized from a bona fide purchaser and returned to its ownership, the purchaser has the right to make a civil claim against the convicted person for damages caused by the seizure of property.

1307. The protection of the rights of bona fide third parties is provided by CPC Article 414(3), which gives them the right to appeal against the court sentence in the part that affects their rights and interests.

1308. Criterion 4.4 – (Mostly met). Mechanisms of seizure, accounting, storage, transfer, and use (including disposal) of physical evidence and confiscated property are regulated by RK Government Resolutions No. 1291 dated December 9, 2014, and No. 833 dated July 26, 2020. These resolutions regulate in detail the mentioned issues regarding money and other valuables, movable and immovable property, and items, the civil circulation of which is restricted or prohibited (narcotic drugs, psychotropic substances, weapons). However, these government acts do not contain provisions regarding the management mechanisms for VA and complex assets.

Weighting and Conclusion

1309. The Republic of Kazakhstan established legal grounds for confiscation of indirect proceeds of criminal offences, introduced directly applicable norms ensuring confiscation of property owned by third parties, monetary equivalent, provided protection of rights of bona fide purchasers, introduced a procedure for confiscation of criminal property when a conviction cannot be secured.

1310. The procedure for the evaluation of property subject to confiscation at the pre-trial stage is not regulated in detail by the legislation.

1311. Freezing (suspension of transactions with funds or other assets) is not applicable to criminal cases of predicate offences (except TF).

1312. The legislation contains no provisions regarding the mechanisms of management of the VA, as well as complex assets.

1313. **Recommendation 4 is rated Largely Compliant.**

Recommendation 5 – Terrorist financing offence

1314. In the 2011 MER, the Kazakhstan was rated "PC" with SR II. As the main deficiencies, the experts noted that the TF offence was not the provision of funds to terrorists or terrorist organizations without the intent to carry out terrorist activities or not related to a specific terrorist act; there were deficiencies in the criminalization of illegal actions against fixed platforms located on the continental shelf and reporting of knowingly false information endangering the safety of a floating vessel; there were no criminal and administrative liability of legal persons.

1315. In addition to the new laws on criminal and administrative liability, Laws No. 63-V dated January 8, 2013, No. 233-V dated July 4, 2014, No. 244-V dated November 3, 2014, No. 403-V dated November 16, 2015, No. 325-V dated May 13, 2020 were amended and supplemented in Law 416.

1316. **Criterion 5.1 –**TF is criminalized on the basis of the UN Convention for the Suppression of the Financing of Terrorism as a separate corpus delicti (CC Article 258). For the purposes of criminal liability, the financing of terrorist (extremist) activity is considered as a special form of abetting terrorism (extremism). It is understood as providing or raising money and (or) other property, rights to property or property benefits, including gifts, exchanges, donations, charitable assistance, providing information and other services or financial services to a natural person or group of persons, or a legal person. Based on the disposition of the analyzed regulation, a mandatory element of the offence is the offender's awareness of: i) the terrorist (extremist) nature of the activities of persons (group of persons); ii) the fact that the provided property and services will be used for terrorist (extremist) activities; iii) or the fact that such property and services will be used to support a terrorist (extremist) group[63], organization, illegal paramilitary formation. This definition corresponds to the "financing of terrorist activities" definition contained in Law 416.

1317. The definition of a terrorist act, as well as the offences categorized as terrorist acts under CC Article 3, encompasses all of the acts set out in Article 2, Par. 1 of the UN Convention for the Suppression of the Financing of Terrorism.

1318. **Criterion 5.2 –**The crime committer under CC Article 258 is any natural person, 14 years of age or older at the time of the offence, who has in any way provided or raised funds for the purpose of:

a) the use for terrorist activities, which in the context of Law 416, Article 1 includes organizing, planning, preparing and carrying out an act of terrorism;

b) provision of support to a terrorist group or organization. Besides that, the criminal law includes provision or raising of funds, provision of financial and other services to a natural person in the awareness of the terrorist nature of his activities. Therefore, the TF acts are financing terrorist organizations or individual terrorists, including without the purpose of financing the commission of a specific terrorist act.

1319. At the same time, according to the definition of a terrorist organization in Article 1 of Law 416, it is an organization that carries out terrorist activities or recognizes the possibility of using terrorism in its activities, in respect of which a court decision recognizing it as terrorist has been made and entered into legal force. Based on the principle of the priority of international treaty provisions over national legislation stipulated by Article 2 of Law 416, organizations designated in the UN sanction lists are equated with terrorists.

1320. In this regard, the financing of an organization that is in fact a terrorist organization, but for which there is no court decision legally stating this fact, and which is not designated in the UN sanction lists, does not constitute TF.

1321. Both direct TF (provision or raising of money, other property, rights to property or property benefits) and indirect TF (provision of financial, informational and other services) are criminalized.

1322. **Criterion 5.2bis –**According to Law 416, Article 1, terrorist activities include: i) organizing, planning, preparing, financing and carrying out an act of terrorism, as well as informing or otherwise

[63] The term "terrorist group" means an organized group with the goal of committing one or more terrorist offences (Article 1 of the Law dated July 13, 1999, CC Article 3).

abetting such acts; ii) inciting an act of terrorism; iii) organizing an illegal paramilitary formation, criminal community (organization), organized group for the purpose of committing an act of terrorism, as well as participation in such organizations; iv) recruiting, arming, training and using terrorists; v) propaganda of terrorist ideas, dissemination of terrorist materials; providing financial, legal or other assistance to terrorists, as well as to organizations whose activities are recognized as terrorist in accordance with the RK legislation, knowing that the said actions will be used to carry out terrorist activities or to support a terrorist organization.

1323. The list of acts falling under the definition of terrorist activity was supplemented in Law 131-VII (entered into force on September 5, 2022). It also includes mercenarism, training of persons for the purpose of organizing terrorist activities and undergoing terrorist training, including traveling to the place of training for participation in terrorist activities.

1324. In the context of this definition, TF offenses include the financing of persons traveling from their country of residence (nationality) to another country for the purpose of committing, planning, preparing, participating in terrorist acts, as well as providing terrorist training (that is, providing training to others) or receiving terrorist training.

1325. The objective aspect of the acts provided for by CC Article 170 (mercenarism) establishes liability for training, financing or other material support of a mercenary, as well as for his use in hostilities, where the financing of a mercenary means providing mercenaries, and possibly their families, with money, and other material support of mercenaries means their outfitting with seasonal clothing, provision of food, appropriate weapons and ammunition, and also with vehicles or other means of transport (tickets), organization of bases for training and education of mercenaries, etc.

1326. **Criterion 5.3 –**The disposition of CC Article 258 does not contain restrictions (obstacles) in terms of criminal assessment of providing or raising funds from any sources as TF. Therefore, the subject of the offence may be money and property obtained both legally and illegally.

1327. **Criterion 5.4 –**According to CC Article 258, TF is not only understood as raising or provision of funds directly for their use in terrorist activities, but also these actions in the awareness of the terrorist nature of the activities of persons, as well as aimed at supporting a terrorist group (organization).

1328. According to the clarifications contained in the RK SC Regulatory Resolution on Certain Issues of Judicial Practice on the Application of Legislation on Terrorist and Extremist Offences dated December 8, 2017, TF includes the provision or collection of uniforms, clothing and gear, communications equipment, medicines, residential or non-residential premises and transportation means. At the same time, for the purposes of criminal liability, the actual use of these assets for the purposes set out in the disposition of CC Article 258 is not required. Therefore, TF does not require that the funds and other property be: a) actually used to perform or attempt to perform an act of terrorism; b) connected with a specific terrorist act.

1329. **Criterion 5.5 –**The offence stipulated by CC Article 258 belongs to the category of intentional[64]. In accordance with the provisions of the RK CPC (Articles 113, 111), the establishment of the form of guilt, i.e. the presence of intent, is part of the fact to be proven in a criminal case, and is carried out on the basis of objective factual data.

1330. **Criterion 5.6 –**Pursuant to the Criminal Code, TF offences are categorized as serious crimes. According to CC Article 258(1), TF offences are punishable by imprisonment for a term of 5 to 9 years with confiscation of property. TF committed (i) repeatedly; (ii) or by a person exercising the powers vested in him by virtue of his office, or a person who performs managerial functions in a commercial or other organization, or the leader of a public association; (iii) or by a group of persons by prior conspiracy; (iv) or on a large scale – is punishable by imprisonment for a term of 7 to 12 years with confiscation of property. The sanctions for TF against natural persons are proportionate and dissuasive.

[64] According to CC Article 20, an act is recognized as intentional if a person was aware of the public danger of his actions, foresaw the possibility or inavoidability of socially dangerous consequences and wished them to occur (direct intent) or consciously allowed or treated them indifferently (indirect intent).

1331. The criminal law (note to CC Article 258) contains a rule on exemption of a natural person from criminal liability for TF in cases of committing a crime under threat of violence and voluntarily reporting its commission, as well as actively contributing to the detection or suppression of an offence (provided that the actions of the guilty person do not contain elements of another offence). These provisions are aimed at stimulating positive post-criminal behavior of the guilty persons, detection and suppression of TF and terrorist offences. Taking into account the reservations on the application of this regulation, the experts believe that it does not establish excessively broad grounds for exemption from criminal liability for TF. In this regard, the mentioned provisions of the law are not considered by the experts as affecting the assessment of sanctions for TF.

1332. **Criterion 5.7 –**In accordance with the fundamental principles of national legislation, criminal liability of legal persons in the Kazakhstan is not applicable. Administrative liability of legal persons is stipulated by the CC, but administrative liability of legal persons is not established directly for TF. CAO Article 214 refers to administrative offences breaches of the AML/CFT legislation by the obliged entities (for more details, see Recommendation 35).

1333. According to Law 416, Article 21, the activity of organizations, as well as their structural subdivisions, is prohibited by recognizing it as terrorist and liquidating in the manner prescribed by law. Upon liquidation of such an organization, all its property located in the territory of Kazakhstan is forfeited to the state. In accordance with the provisions of the Kazakhstan Civil Procedure Code, the decision to recognize an organization as a terrorist organization and to confiscate its property shall be made by the court at the prosecutor's request in civil proceedings. Liquidation of legal persons through civil proceedings does not prevent natural persons from being held criminally liable for TF. Thus, in relation to legal persons only civil liability for TF is stipulated, with the only sanction being liquidation, which entails the confiscation of property. This sanction is dissuasive, but the lack of variability of sanctions does not allow to conclude about its proportionality.

1334. **Criterion 5.8 –**Kazakhstan criminal legislation recognizes as crimes: (a) preparation and attempt to commit a crime (CC Article 24), i.e. attempt to commit a crime; (b) complicity in a crime, including intermediation (CC Article 28); (c) organization and instigation to a crime (CC Article 28); (d) repeated commission of a crime by a group of persons by prior conspiracy (CC Article 258(2)).

1335. Criminal liability for complicity in a crime or for an incomplete crime is incurred under CC Article 258 with reference to Articles 22, 28, respectively, for the purposes of qualification and determination of the term of punishment. Besides that, the Kazakhstan criminal law criminalizes the unauthorized concealment of a serious crime, including TF (CC Article 432).

1336. **Criterion 5.9 –**Since the country considers any offence included in the Criminal Code to be a predicate offence for ML if criminal proceeds are derived from it, the terrorist financing offence (CC Article 258) is a predicate offence.

1337. **Criterion 5.10 –** The CC establishes the universal principle of territorial extent of criminal law. According to CC Article 8(2), its provisions apply regardless of the location of terrorist offences to which TF belongs. This means that TF is a criminal offence regardless of whether the person who committed it is in the same country as terrorists (terrorist group, organization) or where a terrorist act is planned (carried out) or in another country. That is, the financing of terrorist activities carried out outside the territory of the Kazakhstan is as much an offence as the financing of terrorist activities in the territory of the Kazakhstan. In cases where TF is committed outside of the territory of the Kazakhstan, the offenders can be prosecuted under the CC in cases where they are prosecuted in the Kazakhstan and they were not prosecuted for the said act in the territory of a foreign jurisdiction (CC Article 8).

Weighting and conclusion

1338. Kazakhstan does not criminalize the financing of terrorist organizations that have not been recognized as such by a court or that are not designated in the UN sanction lists. The liability of legal persons is limited to their liquidation through civil proceedings, such sanction is not proportionate in all cases.

1339. **Recommendation 5 is rated Largely Compliant.**

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

1340. In the 2011 MER, the Kazakhstan was rated "Partially Compliant" with the requirements related to the freezing of funds used for terrorist financing (former SR.III). The main deficiencies included the following: the existing regime of suspension of transactions and the use of criminal procedural mechanisms in relation to persons designated in the terrorist list raises questions about the effectiveness of implementing Resolutions 1267 and 1373; lack of effective laws and procedures to examine and implement, if appropriate, measures initiated under freezing mechanisms in other jurisdictions; lack of authority for the FIU to communicate the measures taken under freezing mechanisms; lack of clear guidance for FIs to take action if a transaction involving designated persons is identified; lack of de-listing procedure for those designated in the lists of persons involved in terrorism and extremism; lack of mechanisms to allow access to the portion of funds that is necessary for basic expenses in accordance with UNSCR 1452. Besides that, there were no sanctions for not suspending a suspicious transaction – both administrative and criminal.

1341. **Criterion 6.1 –**Designation of persons in accordance with UNSC Resolutions 1267/1989/2253 and 1988:

a) MFA is the body responsible for the representation of Kazakhstan in international organizations, coordination of international activities of government authorities, conduct of affairs with international organizations (RK Government Resolution No. 1118 dated October 28, 2004).

   The NSC prepares proposals of the Kazakhstan on listing (de-listing) individuals and entities designated in the national TF list to the UNSC Committees' sanction list according to the forms established by them (Par. 28 and 29 of Order 1009/dsp) and sends the above information to the MFA with notification of the GPO.

   MFA is the competent agency responsible for sending proposals on persons and entities prepared by Kazakhstan to the UNSC Committees 1267/1989 and 1988 for designation in the UNSC Consolidated Sanctions List (Regulations of the MFA, Par. 30-1).

b) National legislation provides for a procedure for identifying individuals and entities for designation in the lists generated by the UNSC Committees under the relevant Resolutions. Nominations of a person to the UNSC may be made on the basis of a national listing carried out in accordance with UNSCR 1373. Applications for nomination shall be prepared using the forms established by the UNSC Committees (Order 1009/dsp, Par. 28).

c) The designation of an entity or an individual in the national TF list is carried out if there are the grounds provided for in Article 12, Par. 4 of the AML/CFT Law. In accordance with the provisions of Order 1009/dsp, the NSC prepares proposals of the Kazakhstan on listing (de-listing) of individuals and entities designated in the national TF list in (from) the UNSC Committees' sanction lists. Kazakhstan legislation does not currently have a procedure for selecting names to be designated in the UNSC Committees' sanction list. The Kazakh authorities stated that the process for identifying persons is based on a standard of "reasonable basis" or "reasonable grounds" for designating proposed names in the UNSC Committees' sanction list, and that no conviction in a case is required to propose a name for filing such proposal for designation.

d) Proposals to the relevant UNSC Committees are prepared by the NSC according to the forms established by these Committees followed by submission of this information to the MFA with notification of the GPO (Order 1009/dsp, Par. 28).

e) The procedure for submission by the Kazakhstan of proposals to the steering UNSC Committees and the content of the submitted information, as well as the criteria and grounds for disclosure of the state status when submitting proposals are determined by the provisions of Order 1009/dsp. According to the competent authorities of the Kazakhstan, the issue of disclosure of the status of the

Kazakhstan as a state that made proposals for designation in the sanction list is considered on a case-by-case basis.

1342. **Criterion 6.2 –**Designation of persons in accordance with UNSCR 1373:

a) **(met)** The FMA is responsible for making a list of entities and individuals involved in the financing of terrorism and extremism (hereinafter the national List). The grounds for designation in the national List, in accordance with AML/CFT Law, Article 12, Par. 4, are as follows:

- a sentence of a court of the Kazakhstan, which came into force, declaring a person guilty of committing extremist and (or) terrorist offences;
- lists of entities and individuals involved in terrorist and extremist activities (based on the data provided by law enforcement and special government authorities), generated by GPO;
- a decision of a court of the Kazakhstan, which has entered into legal force, to recognize an entity as a terrorist or extremist organization, as well as its liquidation in connection with terrorist activity or extremism;
- sentences (decisions) of courts and other competent authorities of foreign states recognized in Kazakhstan with regard to entities or individuals carrying out terrorist activities;
- designation of an entity or individual in the list of persons involved in terrorist organizations or terrorists compiled by international counter-terrorism organizations or their authorized bodies;
- application of targeted financial sanctions to an entity or individual in accordance with the UNSC Resolutions and/or designation of an entity or individual in the sanction lists of the steering UNSC Committees based on Resolutions in the sphere of combating terrorism and its financing.

b) In accordance with AML/CFT Law, Article 12, Par. 2 and Par. 6(4), the FMA receives the information necessary for the formation of the national list from the MFA, GPO, authorized state statistics body. Besides that, according to AML/CFT Law, Article 12, Par. 4(4), sentences (decisions) of courts and decisions of other competent authorities of foreign states in relation to entities and individuals involved in terrorist activities are the basis for designation of such entities and individuals in the national TF List. The designation of entities or individuals in the national TF list (including at the request of a foreign state) is subject to the grounds stipulated by AML/CFT Law, Article 12, Par. 4. The procedure and mechanism of verification of requests for designation in the national TF list received from other states are regulated by Order 274, Par. 24-29 as well as Par. 11 and 13 of the Regulations of the FMA No. AFM-15-8-0/819 dated August 31, 2022.

c) The incoming request from the competent authority of a foreign state about the possible involvement of an entity or an individual in terrorist activities is considered by the FMA within 20 minutes (Order 274, Par. 23 and 25), and, if there are grounds for designation in the List, the indicated persons are included for a period of up to 15 calendar days in the temporary list – "the list of persons involved in terrorist activities" (AML/CFT Law, Article 12, Par. 10, Order 274, Par. 26), which is published on the official website (and in personal accounts) for the obliged entities to take appropriate measures to freeze assets. The competent authorities within 15 calendar days make a decision on the sufficiency of the grounds for designation in the TF List. Lists are included in the section "designated" on the FMA Internet resource for up to 15 calendar days for further coordination with the GPO and NSC authorities, as well as possible sending of a clarifying request to a foreign country. In case of approval, these persons are moved to the section "active".

The provisions of AML/CFT Law, Article 12, Par.10 apply, inter alia, to foreign state requests submitted to the FMA under the EAG Mutual Freeze Project. If a foreign state's request for freezing funds is received through the MFA, it is included in the national list pursuant to AML/CFT Law, Article 12, Par. 2. If the relevant request is received by the GPO, law enforcement or special

government authorities, the entities and individuals are designated in the list compiled by the GPO and are also designated in the national list in accordance with AML/CFT Law, Article 12, Par. 2.

d) The grounds for designation in the national list, in accordance with AML/CFT Law, Article 12, Par. 4, is the a criminal prosecution for terrorist activities and are also the suspecting the involvement of a person in terrorist activities based on the materials of LEAs/SSSs (Order 1009/dsp, Par. 22).

e) In accordance with the provisions of Order 274, Par. 30, the FMA, in consultation with the Kazakhstan competent authorities, shall annually compile lists of persons involved in terrorist activities in the Kazakhstan to submit requests to foreign states for application of asset freezing measures. Identification data on persons and organisations whose information is sent to foreign countries includes: name, surname, patronymic (if any), individual identification number, identity document, passport data, information on participation in legal entities, branches and representative offices, information on property, grounds for inclusion in the list (Order 1009/dsp, Annex 9). Such cooperation may also be carried out on the general principles of reciprocity under AML/CFT Law, Article 19-1, Par. 2 or in accordance with the Kazakhstan international treaties.

1343. **Criterion 6.3 –**

a) The FMA receives information from government authorities of the Kazakhstan to designate the person or organisation on the national TF list (AML/CFT Law, Article 12 and Order 274, Par. 5). Since February 2017, the FMA is connected to the automated databases of other government authorities, which allows receiving information from the information exchange system of law enforcement and special government authorities, as well as other bodies, with the right to access 36 services (Annex 1 to Order of General Prosecutor No. 18 dated February 22, 2017 and the Minister of Finance No. 127 dated February 22, 2017). When necessary to clarify the information it receives, the FMA uses existing databases or requests the appropriate government authority. Besides that, the FMA has access to the information systems of the Tax Committee and remote access to the Information System of the Committee on Legal Statistics and Special Accounts of the GPO, the database of the Border Service of the NCS, and receives on a quarterly basis information on the movement of cash and other highly liquid financial instruments across the state border.

b) The FMA operates without prior notice to entities and individuals proposed for designation, i.e., it operates *ex parte*.

1344. **Criterion 6.4 –**According to AML/CFT Law, Article 13, Par. 1-1, not later than twenty-four hours from the date of publishing on the FMA website the information about the entity or individual designated in the List, as well as the temporary list of persons involved in terrorist activities, the obliged entities are required to take immediate measures to freeze transactions with funds or other assets.

1345. According to Article 12 par 2 of the AML/CFT Law the FMA receives the relevant UNSC lists directly. In addition, the MFA additionally informs the FMA of any changes to the UNSC lists (Par. 30 of Order 1118). In order to ensure the urgency of measures to freeze assets of persons on the UNSC sanctions lists, the FMA has developed and approved a number of regulations, in particular Oder 5 dated 21.06.2021 and Order 274 dated 22.08.2021. Thus, Order 5 approves the procedure of forming the list by the responsible officer of the FMA upon receipt of information on any changes to the UNSC list. Upon receipt of the notification to the e-mail of the head and employees of the FMA subdivision on inclusion of an organization or a natural person on the UN Security Council sanctions lists, an employee of the FMA subdivision responsible for inclusion of the changes to the List shall immediately (within 3 hours) make such changes independently and within 20 minutes publish it on the official website and send information to the concerned government authorities and organizations via the electronic document flow, personal account, e-mail and cell phones via messengers (AML/CFT Law, Article 12, Par. 1, Order 5 Par. 7 and Order 274, Par. 8, 14). In addition, in 2022, FMA also amended its internal regulations to ensure that changes to the list are fully automatic following the publication of UNSC decisions.

1346. The procedure for the establishment of the list on weekends and public holidays is the same as

described above (Paragraphs 7 and 8 of Order 5). To ensure the urgency of action to freeze the assets of persons on the UNSC sanctions lists on weekends and public holidays, the First Deputy Head of the FMA approves (signs) a duty schedule on a monthly basis (Order 5 Par. 5 and Order 9 dated 11.03.2021).

1347. The national list is formed by the responsible FMA officer within a few hours of the receipt of information from the Information System of the Committee on Legal Statistics and Special Accounts and/or GPO, as well as the request of the competent authority of a foreign state (Order 1009/dsp, Par. 22 and Order 274, Par. 8).

1348. **Criterion 6.5 –**

a) According to AML/CFT Law, Article 13, Par. 1-1, not later than twenty-four hours from the date of publication on the FMA website of information about the designation of an entity or an individual in the List, as well as the temporary list of persons involved in terrorist activities, the obliged entities are required to take immediate action to freeze transactions with funds or other assets. At the same time, the obligation to apply freezing measures does not apply to all natural and legal persons, but only to FIs and DNFBPs, since the legislation of the Kazakhstan has no provisions directly stipulating liability for violation by all natural and legal persons of the ban on providing funds and other assets to the designated persons.

   The current legislation also provides for other measures to freeze the assets of persons designated in the List:

   - refusal to perform state registration of legal persons (Law 2198, Article 11, Par. 4-1);
   - prohibition to be a founder (participant) of a non-profit organization (Law 142-II, Article 20, Par. 3);
   - refusal to perform registration of rights to immovable property (Law 310-III, Article 31, Par. 1(1-1));
   - refusal to perform registration actions with respect to vehicles (Law on Road Traffic, Article 68, Par. 1 (6-1));

   The current legislation provides for the obliged entities to notify their clients of the application of asset freezing measures to them on the basis of the designation of such clients in the List (AML/CFT Law, Article 11, Par. 5).

b) Obligation to freeze assets. The AML/CFT Law does not contain the term “funds or other assets”. However, this term is defined in other normative acts. In accordance with Article 115 of the Kazakhstan Civil Code, property includes: items, money, including foreign currency, financial instruments, works, services, objectified results of creative intellectual activity, trade names, trademarks and other means of products identification, property rights, digital assets and other property. According to Article 117 of the RK Civil Code, property is divided into immovable (land plots, buildings, facilities, perennial plantations and other property) and movable (money, securities, other property). Subsoil, waters, flora and fauna, other natural resources belong to the state property, other property, including land and strategic facilities, may be in private ownership (RK Civil Code, Articles 191-193-1).

   i. In accordance with AML/CFT Law, Article 13, Par. 1-1, not later than twenty-four hours from the date of publication on the FMA website of information about the designation of an entity or individual in the List, as well as the temporary list of persons involved in terrorist activities, the obliged entities are required to take immediate measures to freeze transactions with funds or other assets as follows:

      - suspend debit transactions on bank accounts of designated entity or natural person, on bank accounts of the client, whose BO is designated natural person (except for transactions related to servicing bank accounts), entity directly or indirectly owned or controlled by

designated entity or natural person, as well as natural or legal person acting on behalf or at the direction of designated entity or natural person;

- suspend the execution of instructions for payment or transfer of money without using the bank account of designated entities and natural persons, instructions of the client, whose BO is designated natural person, and the entity, directly or indirectly owned or controlled by designated entity or natural person, as well as the natural or legal person, acting on behalf or at the direction of designated entity or natural person;
- block the securities in the security holders registers and nominal holding record-keeping system on the personal accounts of designated entity or natural person, on the personal accounts of the client, whose BO is designated natural person, and the entity directly or indirectly owned or controlled by designated entity or natural person, and the natural or legal person acting on behalf or at the direction of designated entity or natural person;
- refuse to conduct other transactions with funds and (or) other assets performed by designated entity or natural person or for their benefit, as well as by the client, whose BO is designated natural person or for their benefit (except for crediting money to the bank account of such person, depositing, transferring mandatory pension contributions to the Single Pension Savings Fund), by the entity directly or indirectly owned or controlled by designated entity or natural person or for its benefit, as well as by a natural or legal person acting on behalf of or at the direction of designated entity or natural person or for their benefit.

ii. The obliged entities shall take measures to freeze transactions with funds or other assets (see Subpar. (i)). At the same time, according to AML/CFT Law, Article 1, Par. 3, BO is a natural person who directly or indirectly owns more than twenty-five percent of shares in the authorized capital or outstanding shares (excluding preferred and treasury shares) of the client that is a legal person; who exercises control over the client in another way; for whose benefit the client conducts transactions with funds or other assets. As such, the Kazakhstan has the obligation to freeze funds or other assets that are wholly or jointly owned (or controlled), directly or indirectly, by designated individuals or entities.

iii. The legislation does not establish an explicit obligation to freeze funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or those included in the temporary list of persons involved in terrorist activities.

iv. Similarly to Subpar. (ii), given the existence of the term "BO" in the AML/CFT Law, the obligation to apply freezing measures to entities or individuals acting for or on behalf of persons designated in the List or those included in the temporary list of persons involved in terrorist activities is secured in the country.

c) There is no statutory prohibition for legal or natural persons, other than the obliged entities, to apply measures not to make assets available to persons designated in the List. Certain restrictions on the sale of other assets, other than non-cash funds, by the persons designated in the List are implemented by the government authorities *(see subcriterion (a) of this criterion)*. Besides that, the enforcement by the competent authorities of measures to implement UNSCR 1373 is regulated by Kazakhstan Government Resolution No. 1644 dated December 15, 2001. At the same time, this document does not affects other Resolutions (1267 and 1988).

d) In accordance with Order 274, Par. 14, the FMA is required to provide the list to the obliged entities without delay – within 20 minutes of its amendment (listing/de-listing) by publishing the list on the official FMA website, notifying in the personal account, sending notifications to e-mail addresses and cell phones (via messengers) in order to implement the freezing measures by the obliged entities and individual government authorities (AML/CFT Law, Article 13, Par. 1-1, Order 274, Par. 16).

To improve understanding of the TFS requirements among the obliged entities, the FMA provides an explanation of the legal regulation of this issue on its official website. Besides that, information on the application of TFS is communicated to the obliged entities through personal accounts.

e) In accordance with AML/CFT Law (Article 13, Par. 2) the obliged entities shall submit to the FMA reports on measures for freezing transactions with funds and (or) other assets, attempted transactions and refusals to execute transactions electronically through dedicated communication channels.

f) In accordance with AML/CFT Law (Article 13, Par. 6) the rights of the obliged entities in cases of refusal to conduct transactions, as well as in cases of suspension of transactions with funds and (or) other assets, are not grounds for civil liability of the obliged entities for violation of the terms of the relevant contracts (obligations). Besides that, the suspension and freezing of transactions with funds and (or) other assets are not grounds for civil or other liability of government authorities for damages, including lost profits, arising from such suspension and freezing. Besides that, in the case of providing information, data and documents to the FMA as part of the execution of the AML/CFT Law requirement, the obliged entities and their officials, regardless of the outcomes of the report shall not be liable under the laws of the Kazakhstan, as well as the civil contract (AML/CFT Law, Article 11, Par. 7).

Also, the provision of information, data and documents by a legal entity or foreign unincorporated entity to the authorized body for the purposes and in the manner prescribed by the AML/CFT Law is not a disclosure of official, commercial or other secrets protected by law, except for bank secrecy, and not a violation of the conditions of collection and processing of personal data and other information protected by law (AML/CFT Law, Article 12-3, introduced by Law 131-VII). Despite the fact that the legislation of the Kazakhstan lacks provisions directly protecting the rights of bona fide third parties, the authorities provided the experts with extensive judicial practice, demonstrating cases where the court, guided by the provisions of the Constitution and the Civil Code, protected the legitimate interests of citizens.

1349. **Criterion 6.6 –**

a) MFA is the competent authority responsible for sending proposals by the Kazakhstan on de-listing of persons and entities from the UNSC Committees' lists (Order 1118, Par. 31). In this case, the NSC prepares proposals of the Kazakhstan on de-listing of individuals and entities from the sanction list of the UNSC Committees, according to the forms established by them (Order 1009/dsp, Par. 28).

b) AML/TF Law, Article 12, Par. 5 contains the grounds for de-listing an entity and an individual from the national list.

c) AML/CFT Law, Article 12, Par. 7 provides the procedure for legal and natural persons subject to de-listing from the national TF list to submit a corresponding written motivated application to the FMA, the procedure for consideration of such an application and the possibility to appeal against it. As a result of the appeal, there is a mechanism for reconsidering previously adopted judicial acts (RK CPC, Article 53, Par. 1(4)).

d) Kazakhstan authorities for consideration of requests for de-listing entities and persons from the relevant sanction lists by the UNSCR 1988 Committee use the established procedures and processes, published on the UNSCR 1988 Committee website. An individual on the UNSC list may submit an appropriate application to the FMA (par. 2.1, 3.1 and 3.2 of FMA 08-2-0/8002-vn dated 07.09.2022). In addition, the FMA has developed and approved a guidance for persons on the UNSC lists. This guidance is available on the official website of the MFA and FMA.

e) The publicly known procedures to inform those designated in the Al-Qaida-related Sanction List about the applications for de-listing submitted to the UN are similar to those described in *paragraph (d).*

f) AML/CFT Law, Article 12, Par. 7 provides for the procedure for submission by entities and individuals, erroneously designated in the List, the corresponding written motivated application to the FMA, the procedure for consideration of such an application and the possibility to appeal against it. As a result of the appeal, there is a mechanism for reconsidering previously adopted judicial acts (RK CPC, Article 53, Par. 1(4)). A same mechanism is used in cases of "false positives".

g) FMA shall publish the de-listing decision on its website without delay, but not later than one business day from the date of such decision, and forward it to the relevant government authorities and organizations (AML/CFT Law, Article 12, Par. 5-1, introduced by Law 131-VII, Order 274, Par. 11). De-listing from the TF-related List is grounds for revoking the application of freezing measures (AML/CFT Law, Article 12, Par. 8). The procedure for unfreezing funds and other assets is regulated by Order 274, according to which the obliged entities upon receipt of information about the de-listing of an entity or an individual from the TF-related List shall take steps to unfreeze the funds or other assets owned by them without delay.

1350. **Criterion 6.7 –**For persons included in the national List in accordance with UNSCR 1373, AML/CFT Law (Article 12, Par. 8) provides for a procedure for applying to the obliged entity to conduct – in order to secure own livelihood and that of family members who do not have independent sources of income – transactions related to receiving wages or work leave in the amount of the minimum wage (for each family member), making social payments, as well as obligatory payments to the budget. The rules for payment of such funds are approved by Order of the Ministry of Finance No. 613 dated December 4, 2015.

1351. With regard to persons designated in the sanction lists under UNSCR 1267, 1989 and UNSCR 1452, AML/CFT Law Article 12, Par. 8-1 provides for procedures for application to the FMA by these persons, consideration of their applications on partial or full cancellation of applied measures to freeze transactions with finds and/or other assets (supported by the FMA) by the relevant UNSC Committee followed by informing the obliged entity, as well as the applicant, about the decision taken without delay (but not later than one business day from the receipt of a favourable decision of the UNSC Committee or international counter-terrorism organization.

1352. All transactions of access to frozen funds are subject to accounting on the basis of reports submitted by the obliged entities to the FMA (reporting on freezing measures is stipulated by AML/CFT Law, Article 13, Par. 1-1, suspicious transactions reporting – by Article 13, Par. 2 of the above Law).

Weighting and conclusion

1353. Kazakhstan generally complies with its obligations to apply TF-related TFS through their inclusion in the AML/CFT Law as well as in the relevant regulations. However, there is a deficiency: the legislation does not contain legally binding requirements covering all natural and legal persons (not only FIs and DNFBPs), which relate to the freezing of funds or other assets, as well as the prohibition to provide funds/assets/services to natural or legal persons designated in the sanction lists.

1354. **Recommendation 6 is rated Partially Compliant.**

Recommendation 7 – Targeted financial sanctions related to proliferation

1355. This is a new Recommendation that was not assessed in the 2011 MER. In context of this Recommendation, the AML/CFT Law (Law 191-IV) together with the Regulation on maintaining the list of entities and individuals linked to terrorism, extremism and proliferation financings and freezing or unfreezing transactions with funds and (or) other assets (adopted by the FMA Order 274 dated August 22, 2022) apply.

1356. **Criterion 7.1 –**The procedures of application of targeted financial sanctions against entities or individuals linked to proliferation financings (PF-related TFS) are set out in the AML/CFT Law Art.12-1 and Art.13, Par.1, subpar.1-1. FMA is responsible for implementation of PF-related targeted financial sanctions. For this purpose, entities and natural persons that are subject to targeted financial sanctions under

the UNSC Resolutions related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing are included in the national List of entities or individuals linked to proliferation financing (national PF List) compiled and maintained by the FMA (AML/CFT Law Art.12-1, Par.2).

1357. The following procedure is established to ensure that assets of designated persons included by the UNSC Committees in the PF-related sanction lists are frozen without delay. The head and the executive officer of the FMA special unit are subscribed to notification about listing/delisting of persons and entities on the web-platform of the UNSC Committees and are notified by e-mail of any changes in these lists. Upon receipt of the notification to the e-mail of the head and employees of the FMA subdivision on inclusion of an organization or a natural person on the UN Security Council sanctions lists, an employee of the FMA subdivision responsible for inclusion of the changes to the List shall immediately (within 3 hours) make such changes independently and within 20 minutes publish it on the official website and send information to the concerned government authorities and organizations via the electronic document flow, personal account, e-mail and cell phones (via messengers). In addition, in 2022, FMA also amended its internal regulations to ensure that changes to the list are fully automatic following the publication of UNSC decisions.

1358. The procedure for the establishment of the list on weekends and public holidays is the same as described above (Paragraphs 7 and 8 of Order 5). To ensure the urgency of action to freeze the assets of persons on the UNSC sanctions lists on weekends and public holidays, the First Deputy Head of the FMA approves (signs) a duty schedule on a monthly basis (Order 5 Par. 5 and Order 9 dated 11.03.2021).

1359. Within 24 hours following publication of information about inclusion of an entity or individual into the national PF List on the FMA official website, obliged entities take measures to freeze transactions with funds or other assets of their customers (AML/CFT Law Art.13, Par.1, subpar.1-1).

1360. **Criterion 7.2 –**

a) Within 24 hours following publication of information about inclusion of an entity or individual into the national PF List on the FMA official website, obliged entities take measures to freeze transactions with funds or other assets of their customers (AML/CFT Law Art.13, Par.1, subpar.1-1).

   Besides that, the applicable legislation provides for application of other measures for freeing assets of persons included in the national PF List, such as:

   - Denial of state registration of legal entities (Law 2198 Art.11, Par.4-1);
   - Prohibition from being founders (members) of non-profit organizations (Law 142-II Art.20, Par.3);
   - Denial of state registration of ownership title to real estate property (Law 310-III Art.31, Par.1, subpar.1-1);
   - Denial of registration of transport vehicles (Law on Road Traffic Art.68, Par.1, subpar.6-1);

   However, the legislation does not require each and every legal and natural person (and not just obliged entities as provided for in AML/CFT Law Art.13, Par.1, subpar 1-1) take measures for freezing assets of persons included in the List.

b) Asset freezing obligation. The concept of “funds or other assets” is not defined in the AML/CFT Law, but is enshrined in Articles 115 and 117 of the Civil Code.

   i. Pursuant to Article13, Par.1-1 of the AML/CFT Law, obliged entities are required to promptly, i.e. within 24 hours following publication of information about inclusion of an entity or individual into the national PF List on the FMA official website, take measures to freeze transactions with funds or other assets of their customers, including customers that are BO by a person included in the national PF List *(similar to criterion 6.5 (b))*.

ii. Given that the Kazakhstan legislation requires obliged entities to take freezing measures in respect of customers BO by persons included in the national PF List and also in respect of entities directly or indirectly owned or controlled by persons included in the national PF List and natural or legal persons acting on behalf or at the direction of persons included in the national FP List, Kazakhstan has implemented the obligation related to freezing of funds and other assets directly or indirectly controlled by persons included in the national PF List.

iii. Kazakhstan legislation imposes no explicit obligations to freeze funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by persons included in the national PF List.

iv. Given that the Kazakhstan legislation requires obliged entities to take freezing measures in respect of customers BO by persons included in the national PF List, Kazakhstan has implemented the obligation related to freezing of funds and other assets of entities or natural persons acting on behalf or at the direction of persons included in the national FP List.

c) The legislation does not require each and every legal and natural person (apart from obliged entities) to take measures to prevent assets from being made available to persons included in the national PF List. However, certain restrictions on the use of assets other than cashless funds by persons included in the national PF List are imposed by other government authorities *(see paragraph (a) of this criterion)*.

d) FMA informs obliged entities about decisions of the UNSC to impose TFS under the UNSCR related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing *(see criterion 7.1)*.

Order 274 establishes the procedure of freezing transactions with funds and (or) other assets by obliged entities, government authorities and institutions. In particular, it requires obliged entities to screen transaction parties against the national PF List and to suspend, without delay and prior notice, transactions with involvement of individuals and entities included in the national PF List and (or) freeze funds or other assets owned by them.

In addition to publishing and disseminating the list of PF-related TFS, the FMA also publishes additional information (guidance, typologies) on the application of PF-related TFS on its official website and in personal accounts.

e) Pursuant to Article13, Par.2 of the AML/CFT Law, obliged entities are required to file with the FMA electronic reports about frozen transactions with funds and (or) other assets, attempted transactions and refusals to execute transactions via the dedicated communication channels.

f) According to Article13, Par.6 of the AML/CFT Law, refusal by obliged entities to carry out transactions as well as suspension of transactions with funds and (or) other assets do not entail civil liability of obliged entities for breaches of the contractual obligations.

Besides that, suspension and freezing of transactions with funds and (or) other assets do not entail civil or other liability of the government authorities for losses, including lost profits, incurred as a result of such suspension and freezing actions.

Furthermore, in case of provision of information and documents to the FMA in compliance with the requirements set out in the AML/CFT Law, obliged entities are not held liable under the Kazakh legislation and civil law contracts (AML/CFT Law Art.11, Par.7).

Provision by a legal entity or unincorporated foreign entity of information and documents to the designated government agency for the purposes and in a manner set out in the AML/CFT Law does not constitute an unauthorized disclosure of official, commercial or other secrets protected by law (except for bank secrets) and/or a breach of the terms of collection and processing of personal data

and other information protected by law (Art.12-3, Par.6 of the AML/CFT Law added by Law 131-VII).

However, there are no explicit provisions in the legislation that directly protect the rights of bona fide third parties that may be affected as a result of implementation of asset freezing measures in respect of persons that have property obligations to them.

Besides that, there are no explicit provisions in the AML/CFT Law that specifically release obliged entities from liability for application of freezing measures set out in AML/CFT Law (Art.2-1, Par.1-1).

1361. **Criterion 7.3 –**Pursuant to Article 14 of the AML/CFT Law, the government monitoring of compliance by obliged entities with the AML/CFT legislation, including compliance with the statutory requirements related to freezing of transactions with funds and (or) other assets, suspension and denial of transactions that are subject to financial monitoring, and development and implementation of internal control rules, is performed by the relevant government authorities within their respective purview in a manner established by the Kazakh legislation. The corresponding provisions are set out in the sectoral legislation that regulates the powers of such government authorities.

1362. The legislation provides for liability for failure to comply with the AML/CFT legislation as it pertains to application of freezing measures. In particular, according to Article 214 of the Code of Administrative Offences, breaches by obliged entities of the Kazakh AML/CFT legislation requirements related to freezing transactions with funds and (or) other assets and reporting frozen transactions is punishable by a fine in amount of 50 monthly calculated indices (MCI) imposed on natural persons, in amount of 140 MCI imposed on executive officers, notaries, advocates and small businesses, in amount of 220 MCI imposed on medium businesses, and in amount of 400 MCI imposed on large businesses.

1363. The severity of punishment increases in case of repeated breaches. For example, in case of detection of similar breaches committed three or more times during a year after the imposition of administrative sanctions, actions (inactions) of obliged entities entail imposition of a fine in amount of 150 MCI imposed on natural persons, in amount of 300 MCI imposed on executive officers, notaries, advocates and small businesses, in amount of 600 MCI imposed on medium businesses, and in amount of 1200 MCI imposed on large businesses with cancellation or suspension of a license or qualification certificate for up to 6 months or suspension of activity for up to 3 months.

1364. Carrying out activities without registration, authorisation or failure to file report (when required, if such action does not constitute a criminal offence) is punishable under Article 463 of the Code of Administrative Offences by a fine in amount of 15 MCI imposed on natural persons, in amount of 25 MCI on executive officers, small businesses and non-profit organizations, in amount of 40 MCI imposed on medium businesses, and in amount of 150 MCI imposed on large businesses with or without confiscation of instrumentalities of administrative offence.

1365. **Criterion 7.4 –**

a) The applicable legislation does not contain provisions establishing the procedures (and the central authority) enabling entities and individuals included in the national PF List to petition requests for de-listing at the Focal Point.

   However, the UNSC allows natural persons to apply for de-listing directly to the Security Council in accordance with the de-listing procedures set out on the website of the UNSC Focal Point. For this purpose, the national PF List section on the FMA official website contains links to the websites of the relevant UNSC Committees on which the detailed procedures of inclusion into and exclusion from the UNSC Consolidated Sanction List are provided.

b) According to Article 12-1, Par.4 of the AML/CFT Law, persons mistakenly included into the national PF List may apply to the designated government agency with a substantiated written request for de-listing. The designated government agency considers a submitted request and decides either

to de-list a petitioner or to reject the request with substantiation of such denial. A petitioner may appeal against the decision of the designated government agency in court. Infotmation about this procedure is set out in the national PF List section on the FMA official website. A same mechanism is used in cases of "false positives".

c) Article 12-1, Par.5 of the AML/CFT Law provides that a natural person included into the national PF List may apply to the FMA with a substantiated written request for partial or full unfreezing of frozen funds and (or) other assets needed for covering basic expenses of the petitioner and his/her family members that have no other sources of income. The FMA forwards such petition to the relevant UNSC Committee, and if a positive decision is made by the Committee, the FMA immediately, but not later than one business day following the receipt of such decision, communicates it to the petitioner and the relevant obliged entity.

d) FMA shall publish the de-listing decision on its website without delay, but not later than one business day from the date of such decision, and forward it to the relevant government authorities and organizations (AML/CFT Law, Art.12-1, Par.3).

Order 274 provides that exclusion of an entity or an individual from the national PF List constitutes the grounds for cancellation of transaction freezing measures.

With a view to providing guidelines to obliged entities regarding their actions under the existing freezing mechanism, the procedure of freezing transactions with funds and (or) other assets by obliged entities and government authorities and institutions was adopted (Order 274).

1366. **Criterion 7.5 –**

a) According to Article 13, Par.1-1, subpar.1 of the AML/CFT Law, the addition of funds to a frozen account is an exemption from the TFS regime and, therefore, credit transactions are not blocked and are carried out without restrictions. At the same time, all debit transactions as well as other transactions through frozen accounts are blocked/ terminated.

b) Set out in Article12-1, Par.6 of the AML/CFT Law is the following mechanism of dealing with transactions of listed persons carried out under contracts entered into prior to inclusion of such persons into the national PF List. In this situation, obliged entities immediately notify the FMA of such transactions (except for credit transactions). After that, the FMA, within 24 hours following the receipt of such notice, either suspends a transaction for up to 5 business days and communicates its decision to the reporting obliged entity, or does not respond to the received notice within 24 hours, in which case the obliged entity shall proceed with the transaction. Upon making a decision to suspend a transaction, the FMA, within 3 business days, makes a decision either to permit or deny the transactions and communicates its decision to the reporting obliged entity. Upon expiration of a transaction suspension period ordered by the FMA, the transactions shall be carried out.

A decision to permit a transaction can be made subject to the following conditions:

- A contract is not related to any prohibited items, materials, equipment, goods, technologies, assistance, training, financial support, investments, brokerage or services specified in the UNSC documents related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing;
- Payment will not be received directly or indirectly by an entity or a person designated by the UNSC Resolutions related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Upon making a decision to permit a transaction, the FMA immediately notifies the relevant UNSC Committee of the intention to permit the transaction.

Weighting and conclusion

1367. In general, Kazakhstan has complied with its PF TFS obligations by implementing them into the

AML/CFT Law. However, there is one deficiency: Kazakh legislation does not contain legally binding provisions that apply to all natural and legal persons (and not just to financial institutions and DNFBPs) that require them to freeze funds or other assets and prohibit them from making funds/ assets/ services available to natural or legal persons included in the sanction lists.

1368. **Recommendation 7 is rated Partially Compliant.**

Recommendation 8 – Non-profit organizations

1369. In the 2011 MER, Kazakhstan was rated non-complaint with the requirements relating to NPOs (former SR.VIII). The main deficiencies included the following: the NPO legislation was not reviewed for AML/CFT purposes; no regular analysis of the NPO sector to identify TF risks or any AML/CFT awareness-raising activities were conducted; a system for monitoring the activities of larger NPOs did not exist; no special mechanisms for timely exchange of information on NPOs, both at a national and international level, in case of suspicion of ML / FT were available; the range of sanctions for breaches of the law was too narrow and was not used for AML/CFT purposes. Following the review of the 3rd Follow-up Report of Kazakhstan (2015), it was noted that the country had taken measures to address the deficiencies in complying with SR.VIII.

1370. **Criterion 8.1 –**

a) The Ministry of Information and Social Development (MISD) is the government authority responsible for regulation of NPOs. In Kazakhstan, public and religious associations, and branches and representative offices (standalone divisions) of foreign and international non-profit organizations fall within the FATF definition of NPO. The 2021 TF/PF NRA exercise, which included assessment of risks in the NPO sector, identified the subsets of NPOs that were most susceptible to TF risks. Religious associations are identified as posing the highest risk, while all other types of NPOs are exposed to lesser risks. The MISD determines and identifies those types of NPOs that are exposed to risk of their misuse of TF purpose by examining their activities and reviewing the information (primary statistics and activity reports collected by the designated state statistics agency and the state revenue authorities) submitted to the NPO Database annually before March 31. The government authorities are required to monitor and review the activities of NPOs within their purview for identifying TF risks, summarize the AML/CFT enforcement practice and make proposals for improvement of the AML/CFT legislation by providing this information, as per the approved form, to the designated government agency on an annual basis within the timelines determined by it (AML/CFT Law Art.18, Par.2, subpar.1-2). In particular, the MISD is tasked with monitoring and reviewing the NPO activities for identifying TF risks and is required to provide the findings to the designated AML/CFT agency. In 2022, a separate assessment of risks of terrorist financing through abuse of NPOs was conducted, and CFT Guidelines for the NPO sector were developed.

b) The AML/CFT Law requires the authorities to conduct the national risk assessment (Art. 11-1). The developed procedure of creation of NPOs and monitoring the activities of NPOs operating in the country enables them to freely pursue their objectives, on the one hand, and to prevent possible involvement in illegal activities, on the other hand. Risks of misuse of NPOs for TF purposes arise primarily from the existing possibility to collect (or) move cash. Non-profit organizations often use poorly controlled methods of raising donations such as: cash deposits into NPOs cash registers or bank accounts, collecting cash into donation boxes, use of bank cards and mobile apps, raising donations through intermediaries who may be temporary employees (such as volunteers and foreign partners) that are rarely subject to a vetting process (fit and proper test). The information collected through the TF risk analysis process shows the intention of criminals to use religious organizations for committing illegal acts.

   The NPO sector is featured by a number of vulnerabilities related to potential misuse of their activities for TF proposes. The main vulnerabilities include the following:

- A large number of temporary employees, where NPOs are unaware of the true intentions employees hired by them. The NPO operation mode makes it difficult to conduct fit and proper tests of temporary employees, especially volunteers and foreign partners;
- The extended logistics networks provide for a wide geographic coverage of the sector enabling NPOs to implement their programs in many areas and regions;
- Some NPOs operate across the globe and, therefore, are able to carry out domestic and international transaction often in the regions or in the vicinity of the regions that are most susceptible to terrorist activities.

The NPO vulnerabilities are described in detail in the 2022 report on assessment of TF risks related to misuse of non-profit organizations.

With a view to mitigating risks of misuse of NPOs for TF purposes in the banking sector (wire transfers without opening bank accounts, use of bank payment cards, money transfer systems, e-wallets, etc.), the ongoing efforts are undertaken to further improve the existing internal control mechanisms. However, monitoring of consistency of NPOs expenditures with the declared goals and objectives remains the main method of mitigating risks of abuse of non-profit organizations for terrorism and extremism financing purposes.

c) The Ministry of information and social development is the designated government authority responsible for maintaining the NPO Database, with the actual work being performed by the MISD Committee for Civil Society Affairs. This Database is generated and maintained for enhancing transparency of NPOs and raising public awareness of their activities. The annual NPO activity reports for inclusion into the Database are submitted as per the approved form not later than on March 31 of each year.

Branches and representative offices (standalone divisions) of foreign and international non-profit organizations operating in Kazakhstan publish annual activity reports, including information about their founders, assets, funding sources and expenses.

According to the presented reports, NPOs are subject to monitoring for identifying potential TF-related risks, which special attention paid to the activities of public associations, foundations, religious associations and branches and representative offices (standalone divisions) of foreign and international non-profit organizations. The codes of suspicious transaction indicators in the NPO sector have been adopted.

According to the findings of the TF NPO SRA, a medium risk level is assigned to charitable and religious organizations.

For safeguarding charitable organizations and religious associations against their potential abuse for TF purposes, the AML/CFT Law requires charitable organizations as well as religious associations soliciting voluntary donations and contributions to take measures for preventing their misuse for TF purposes and to:

- Make payments and money transfers requested by third parties or initiated by religious associations themselves only through obliged entities;
- Provide financial statements concerning completed transactions with funds and (or) other assets and information on identified risks at request of the designated government agency;
- Retain information on carried out transactions with funds and (or) other assets that are subject to mandatory state registration and information on their founders (members) for at least five years.

If charitable organizations and religious associations suspect that they are misused for TF purposes, they must report their suspicions and provide the relevant information to the designated government agency.

According to Article 8(4) of the Charity Law and Article 10(3) of the Law on Religious Activities and Associations a charity organization and religious associations applying for voluntary donations must comply with the requirements established by the Kazakhstan AML/CFT legislation. The AML/CFT Law provides for uniform requirements for the above-mentioned organizations to prevent their use for TF purposes. In this regard the requirements of the AML/CFT legislation are consistent with the requirements of the legislation on religious activities and religious associations, as well as the legislation on charity. In turn, Article 18(2)(1-2) of the AML/CFT Law requires the state authorities of Kazakhstan to analyze and monitor, within their competence, the activities of non-commercial organizations in order to identify risks of terrorism financing, to summarize the practice of applying the AML/CFT legislation of Kazakhstan and to make proposals for its improvement with the annual submission of such information to the FMA.

Thus, the NPO sector is sufficiently covered by the current AML/CFT system, and there is no reason to believe that the legitimate activities of such NPOs, including charitable organizations, are in any way prejudiced. Moreover, under Article 6(2) of the Charity Law, no unlawful state interference in the affairs of charitable entities engaged in charitable activities is permitted.

According to Section 6 of the Financial Services Framework Regulations (FSFR), the AFSA is empowered to request and receive from the supervised AIFC member companies any information about their activities, including information on their customers and customer transactions. The authorized AIFC member companies are required to disclose to the AFSA information concerning any aspects of their activities and to develop and implement the relevant systems and internal procedures for complying with these requirements (FSFR Chapter 2, Section 102, Par.1 and 3). The AFSA may obtain information from the AIFC member companies on behalf of other authorities if an assistance request is received from a government or regulatory authority that exercises powers and discharges functions related to combating money laundering, countering the financing of terrorism or enforcing compliance with sanctions (CO-OP Section 2.2I).

d) The NRA exercise is provided for in the legislation and is conducted once in three years. The NRA duration does not exceed 18 months, and the next NRA is conducted upon expiration of 36 months from the date of commencement of the previous NRA (*see criterion 1.3*).

1371. **Criterion 8.2 –**

a) With a view to streamlining cooperation between the public authorities and NPOs and enhancing transparency and social activities of NGOs, Kazakhstan Prime Minister's Executive Order 159-r dated December 28, 2015 adopted the National Plan for Developing Cooperation between NGOs and Public Authorities for 2016-2020, which was amended in December 2018.

The Concept of Development of Civil Society until 2025 adopted by Kazakhstan Presidential Decree 390 dated August 27, 2020 provides for implementation of a public control and oversight system with a broad and active engagement of NGOs, public councils, expert community and civil society activists, promotion of more active transfer of the state governance functions to the non-government sector, etc.

The MISD Action Plan for Implementation of the Civil Society Development Concept includes the following: improvement of legal regulatory instruments and institutional framework for promoting the development of civil society institutions) includes elaboration of a draft Law on Public Oversight, development of ASAR tripartite (NGO-Business-State) partnership platform, steering the activities of the NPO Cooperation Coordination Council under the MISD and implementation of the NGO Academy project.

The MISD implements the NPO Academy project as part of the NPO grant plan. This project aims to professionalize NPOs activities by creating a system of professional training of representatives of non-government organizations and includes the following:

- Developing a NPO professional development training program (covering 800 NPOs);
- Conducting at least 20 online training workshops for the civil society trainers;
- Preparing training materials and methodological guidelines for the NPO Academy;
- Developing online and mobile training methodology and platform;
- Creating an online and digital training studio (webinars, online training courses, training videos, massive open online courses).

Besides that, the MISD implements another grant project entitled "Supporting Effective Operation of Special kazislam.kz Islamic Web Portal" that was created at the direction of the Head of the State following the 38th meeting of foreign ministers of the OIC member countries. The project is aimed at:

- Clarifying the ideological principles of the state policy in religious sphere;
- Clarifying the traditional Islamic canons, the history of Islam in Kazakhstan and its role in the secular state and society;
- Promoting national traditions and patriotism;
- Raising public awareness of destructive activities (including ideology of different radical and extremist groups and threats they pose to the society);
- Improving effectiveness of the kazislam.kz information and advisory service and positioning the web portal as a reliable source of religious information about Islam for public.

The 2021 NRA findings have been communicated to the NPO sector through a number of meetings and workshops with involvement of the FMA, MISD, other government authorities and international experts.

b) On November 11, 2020 and May 14, 2021, the FMA held online expert meetings (with the use of Zoom platform) with representatives of the NPO sector to discuss potential amendments into the AML/CFT legislation, development of a RBA guidance for the NPO sector and implementation of a risk-based approach in the sector in advance of the FATF mutual evaluation. Apart from the FMA officers, the meeting was also attended by the specialists of the SRC and the MISD Committee for Civil Society Affairs as well as the NPO representatives.

   Based on the FATF Guidance Document (on TF Risks for NPOs), the FMA arranged and held a number of meetings to provide methodological support to the MISD in developing methodological guidelines to be disseminated to the NPO sector (for examination and practical application).

c) The NPO Cooperation Coordination Council operates in Kazakhstan since 2005. The Council was established with the aim of developing the non-government sector and promoting its constructive and effective cooperation with the government authorities. The Coordination Council members include representatives of the central government authorities, local executive authorities, leading national NPOs.

   According to the Coordination Council statute, the Council holds semi-annual meetings to discuss further improvements in the NPO legislation and hear the reports of ministries, agencies and local authorities on execution of the Civil Forum orders and directives.

   However the statutory documents of the Council do not explicitly empower the Council to cooperate with NPOs for developing and improving the advanced methods to address TF risks and vulnerabilities.

d) The AML/CFT legislation (Art. 12-2) includes measures aimed at safeguarding charitable organizations and religious associations against their potential abuse for TF purposes. The NPOs soliciting voluntary donations and contributions are required to take measures for preventing their

misuse for TF purposes and make payments and money transfers requested by third parties or initiated by NPOs themselves only through obliged entities. If charitable organizations and religious associations suspect that they are misused for TF purposes, they must report their suspicions and provide the relevant information to the designated government agency. The codes of suspicious transaction indicators in the NPO sector have been adopted.

1372. **Criterion 8.3 –**As indicated in criterion 8.1I, the Ministry of Information and Social Development (MISD) is the designated government authority responsible for maintaining the NPO Database, with the actual work being performed by the MISD Committee for Civil Society Affairs.

1373. Branches and representative offices (standalone divisions) of foreign and international non-profit organizations operating in Kazakhstan publish annual activity reports, including information about their founders, assets, funding sources and expenses.

1374. According to the presented reports, NPOs are subject to monitoring for identifying potential TF-related risks. These reports contain: information on founders (members); activities over the reporting period; general registration, administrative and contact details; information on employees and volunteers; income and expenses over the reporting period; budget; information of participation in projects; information on branches and representative offices; projects implemented by NPOs and other information.

1375. Apart from these reporting obligations that apply to all NPOs, additional requirements for charitable and religious organizations are set out in the AML/CFT Law.

1376. For safeguarding charitable organizations and religious associations against their potential abuse for TF purposes, the AML/CFT Law (Art.12-2) requires such organizations soliciting voluntary donations and contributions to take measures for preventing their misuse for TF purposes and to:

- Make payments and money transfers requested by third parties or initiated by religious/ charitable organizations themselves only through obliged entities;
- Provide financial statements concerning completed transactions with funds and (or) other assets and information on identified risks at request of the designated government agency;
- Retain information on carried out transactions with funds and (or) other assets that are subject to mandatory state registration and information on their founders (members) for at least five years.

1377. If charitable organizations and religious associations suspect that they are misused for TF purposes, they must report their suspicions and provide the relevant information to the designated government agency.

1378. In practice, the MISD applies a risk-based approach to AML/CFT supervision, but the obligation to use RBA is not enshrined in the legislation.

1379. **Criterion 8.4 –**

a) The Ministry of Information and Social Development is the designated government authority responsible for maintaining the NPO Database, with the actual work being performed by the MISD Committee for Civil Society Affairs. This Database is generated and maintained for enhancing transparency of NPOs and raising public awareness of their activities. The annual NPO activity reports for inclusion into the Database are submitted as per the approved form not later than on March 31 of each year.

   Branches and representative offices (standalone divisions) of foreign and international non-profit organizations operating in Kazakhstan publish annual activity reports, including information about their founders, assets, funding sources and expenses.

   Non-profit organizations are held administratively liable for failure to provide and/or untimely provision and/or provision of inaccurate or knowingly misleading information on their activities (including information about their founders, assets, funding sources and expenses) to the designated government authority responsible for cooperation with and supervision of NPOs.

Besides that, Article 20, Par.3 of Law 142-II states that a person included in the list of entities and individuals linked to proliferation financing and (or) in the list of entities and individuals linked to terrorist and extremist financing under the Kazakh legislation may not be the founder (member) of a non-profit organizations.

Law 2198 (Art.11, Par.4-1) states that the state (record) registration and re-registration legal entities and their branches (representative offices) is denied if a person who is the founder (member) and (or) the director of a legal entity is included in the list of entities and individuals linked to proliferation financing and (or) in the list of entities and individuals linked to terrorist and extremist financing under the Kazakh legislation, except for shares (interest in the authorized capital) confiscated and (or) recovered by a court.

Upon detection of relevant breaches, the local executive authorities issue the administrative offence reports (Code of Administrative Offences Art.489-1).

b) According to the NPO legislation, activities of a non-profit organization may be suspended by a court for three up to six months at a request of the prosecution authorities in case of a breach of the RK Constitution and legislation committed by the NPO or in case of repeated actions conducted by the NPO that go beyond the scope and goals of the activities declared in its charter (Article 42 of Law 142-II).

Guilty natural and legal persons, including executive officers of the government authorities, are held liable for committed breaches of the NPO legislation (Code of Administrative Offences Art.489-1; Law 142-II Art.42, Par.1).

The suspension also applies to its right to use bank accounts with the exception of payments under labor contracts, compensation of losses inflicted as a result of its activities, and payment of fines. If during the suspension period ordered by a court, a non-profit organization rectifies the breaches that caused suspension of its activities, it may resume its operation upon expiration of this period. In case of failure by a non-profit organization to eliminate the committed breaches, the prosecution authorities may apply to court for liquidation of this NPO. A court that ordered a suspension of NPO activities may withdraw this restriction ahead of time if the non-profit organization eliminated the breaches and filed an application with court on that.

Besides that, a breach of the NPO legislation entails a warning, and a repeated breach entails imposition of a fine in amount of 25 MCI or suspension of activities for three months. A breach of the requirements for charitable activities set out in legislation on religious activities and religious organizations is punishable by a fine in amount of 50 MCI imposed on natural persons and in amount of 200 MCI imposed on legal entities with suspension of activities for three months.

Engagement of a religious organization in activities that are inconsistent with its charter is punishable by a fine in amount of 300 MCI with suspension of activities for three months. A repeated breach of the legislation on religious activities and religious organizations committed during a year after imposition of administrative sanctions is punishable by a fine in amount of 200 MCI imposed on natural persons, in amount of 300 MCI imposed on executive officers and in amount of 500 MCI imposed on legal entities with prohibition of their activities.

A breach of the AML/CFT legislation entails imposition of a fine in amount of 50 up to 300 MCI with cancellation or suspension of a license or qualification certificate for up to 6 months or suspension of activity for up to 3 months.

1380. **Criterion 8.5 –**

a) The Interagency Working Group (established by FMC Chairman's Order No.59 dated September 13, 2016) operates in Kazakhstan since 2016. It serves as a platform for coordination of the NPO monitoring efforts. With a view to developing and enhancing the effectiveness of measures aimed at implementation of the national AML/CFT policy and coordinating the ML/TF risk mitigation efforts,

the FMA established the Interagency ML/TF Prevention Council (AML/CFT Law Art.11-1, Par.3) composed of the deputy heads of the government executive, supervisory and oversight authorities (Order 95-nk dated May 14, 2021). The MISD, being the Interagency Council member, may propose freezing of funds and other assets of persons that may potentially be included in the national lists of terrorists.

b) Information presented in R.31 shows that the law enforcement and special government authorities have the capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organizations. However, no information on actually conducted investigations has been provided.

c) In order to enable the government authorities to properly monitor and oversee the NPO activities and operations, non-profit organizations are required to submit information on their activities into the relevant database. NPOs created in form of private institutions and public associations as well as branches and representative offices (standalone divisions) of foreign and international non-profit organizations operating in Kazakhstan submit, not later than on March 31 of each year, the annual activity reports (including information about their founders, assets, funding sources and expenses) to the designated government authority responsible for cooperation with and supervision of NPOs in a manner determined by this designated government authority. NPOs also submit primary statistics and activity reports to the designated state statistics agency and the state revenue authorities (MCS Order No.51 dated February 19, 2016; and Law 142-II Art.41, Par.1, 2 and 5). With a view to accessing information and conducting oversight, the MISD has integrated its database into the MoF database, so that tax authorities can perform off-site review of information indicated in the NPO declarations.

   Chapter 33 of the Criminal Procedure Code authorizes the law enforcement or special government authorities to request necessary documents, records and information. Under Article 18 of the AML/CFT Law, the competent authorities report suspicious transactions identified by themselves to the FMA.

d) The AML/CFT Law (Art.21-2) requires charitable organizations and religious associations soliciting voluntary donations and contributions to take measures for preventing their misuse for TF purposes. If charitable organizations and religious associations suspect that they are misused for TF purposes, they must report their suspicions and provide the relevant information to the designated government agency. However, Kazakhstan has not provided information about mechanisms of taking adequate response actions by the competent authorities.

   Order 13 adopted the codes of suspicious transaction indicators in the NPO sector (1040, 1041, 1046, 3003).

   Article 18, Par.2, subpar.12 of the AML/CFT Law requires the MISD to review and monitor activities carried out by NPOs and report findings to the FMA, but frequency of such reporting is not set out in the laws and regulations.

   According to the FSFR Section 6, the AFSA is empowered to request and receive from the supervised AIFC member companies any information about their activities, including information on their customers and customer transactions. The authorized AIFC member companies are required to disclose to the AFSA information concerning any aspects of their activities and to develop and implement the relevant systems and internal procedures for complying with these requirements (FSFR Chapter 2, Section102, Par.1 and 3).

   The AFSA may obtain information from the AIFC member companies on behalf of other authorities if an assistance request is received from a government or regulatory authority that exercises powers and discharges functions related to combating money laundering, countering the financing of terrorism or enforcing compliance with sanctions (CO-OP Section 2.2I).

1381. **Criterion 8.6 –**The AML/CFT Law provides the legal framework for responding to international requests concerning all issues related to AML/CFT, including requests regarding NPOs suspected of TF or involvement in other forms of terrorist support (AML/CFT Law Art.19-1, 19-2 and 19-4). The FMA, LEAs and special government authorities can obtain the basic, financial or other information about NPOs from their international partners. Such information is obtained at request or is shared under international agreements or based on the principle of reciprocity (AML/CFT Law Art.19-1, Par.2). Depending on a request type (mutual legal assistance requests, requests from foreign justice authorities or requests from foreign FIUs and other competent authorities), the incoming requests are forwarded to the General Prosecutor's Office, the Supreme Court, the FMA, the relevant LEA or special government authority identified as the focal points for responding to international requests.

Weighting and conclusion

1382. Comprehensive information from relevant sources was used to determine the types of NPOs at risk of being used for TF purposes and the level of risk, all necessary legal and regulatory frameworks were in place, including those aimed at systematically informing NPOs of the risks of their involvement in terrorist financing without interference, which was generally consistent with the requirements.

1383. In practice, the MISD applies a risk-based approach to AML/CFT supervision, but the mechanism for its response, as well as that of other concerned government authorities, to the identified threats is not fully defined in the regulations.

1384. **Recommendation 8 is rated Largely Complaint.**

Recommendation 9 – Financial institution secrecy laws

1385. In the previous MER, Kazakhstan was rated largely compliant with former Recommendation 4 due to inconsistent legislation and different terminology defining the same subjects or objects that could be a legal impediment and seriously affect the effectiveness of obtaining information from the obliged entities and cooperation with foreign partners.

Access to information by competent authorities

1386. **Criterion 9.1** – Provision of information by financial institutions to the Financial Monitoring Agency does not constitute unauthorized disclosure of official, commercial, bank or other secrets protected by law (AML/CFT Law Art.11, Par.6). In case of provision of information and documents to the designated government agency in compliance with the requirements set out in the AML/CFT Law, financial institutions are not held liable under the Kazakh legislation and civil law contracts (AML/CFT Law Art.11, Par.7). Furthermore, provision of information by financial institutions to the designated government authority responsible, within its purview, for monitoring compline by FIs with the AML/CFT legislation also does not constitute unauthorized disclosure of official, commercial, bank or other secrets protected by the law (Law 474-II Art.14; Presidential Decree 1271, Par.17; Presidential Decree 428 Par.16). However, the AML/CFT Law does not provide for direct access to information by other government authorities.

1387. The sectoral legislation of some financial institutions (professional securities market participants, commodity exchanges, second-tier banks) also contains the provisions governing the disclosure of information to the designated financial monitoring agency for the purposes and in a manner set out in the AML/CFT Law. However, no similar provisions regulating the disclosure of information by microfinance organizations, postal operators, payment service providers, insurance companies, stock exchange and individual finance lessors are found in the legislation. Access by the designated financial monitoring agency to information held by the single pension savings fund is limited to account statements reflecting individual pension account balance and activity.

1388. The disclosure by the AIFC member companies of ML/TF-related information to the competent authorities is not a contravention of any obligation of secrecy or non-disclosure or of any enactment by which this obligation is imposed (AIFC FR0008 Section 13.7.4). However, the term "competent authority"

is not defined in the AIFC regulations and, therefore, it is unclear whether the competent authorities include the AIFC supervisor and the designated financial monitoring agency.

1389. The sectoral legislation of certain types of financial institutions (second-tier banks, professional securities market participants, commodity exchanges, microfinance organizations) contains the provisions governing access to certain, but not all information constituting bank, commercial or other secrets protected by law by the courts, prosecutors, inquiry and preliminary investigation authorities, criminal prosecution authorities, national security authorities, state security service and state revenue authorities within their respective purview and subject to certain conditions.

Sharing information among competent authorities

1390. The FMA is authorized to request necessary documents, records and information related to transactions with funds or other assets from the Kazakh government authorities responsible for overseeing compliance by obliged entities with the applicable legislation within their purview (i.e. supervisory authorities) that must provide the requested information (AML/CFT Law Art.17, Par.1, subpar.1 and Art.18, Par.1, subpar.1). Furthermore, provision of information and documents related to suspicious transactions by these supervisory authorities does not constitute unauthorized disclosure of official, commercial, bank or other secrets protected by law (AML/CFT Law Art.18, Par.4).

1391. The law enforcement and special government authorities as well as the foreign intelligence agency are authorized, with certain limitations, to request documents and information about transactions that are subject to financial monitoring, and provision of requested documents and information does not constitute unauthorized disclosure of official, commercial, bank or other secrets protected by law (AML/CFT Law Art.18, Par.5).

1392. Dissemination by the FMA of information to the government authorities responsible for overseeing compliance by obliged entities with the applicable legislation within their purview is also provided for in Article 4 of Law 474-II, which states that the supervisory and oversight authorities may obtain, free of charge. Necessary information (*inter alia*, from other government authorities), including information constituting official, commercial, bank or other secrets protected by law.

1393. The FMA may also share information with foreign AML/CFT competent authorities at request and spontaneously (AML/CFT Law Art.17, Par.4, subpa.4; Art.19-2, Par.5; Art.19-3; and Art.19-4). But according to Article 50, Par.3 of the Law on Banks and Banking Activities, persons who have accessed, through exercising their duties, the information constituting banking secrecy, are held criminally liable for disclosing these secrets, except for certain situations which, however, do not include exchange of information with foreign competent authorities. Therefore, in such situation, information can be shared only upon court approval.

1394. The designated government authority responsible for overseeing compliance by financial institutions with the AML/CFT legislation within its purview is authorized to exchange information constituting secrets protected by law under the RK international agreements that provide for sharing confidential information (Law 474-II Art.14-1, Par.4; Presidential Decree 1271, Par.6).However, no such provisions are contained in Presidential Decree 428, which may impede exchange of information with the relevant foreign competent authorities.

Sharing information among financial institutions

1395. Except for the right granted to banks to share among themselves information concerning bank loans provided to customers (Law 2444 Art.50, Par.4, subpar.10), the legislation contains no other provisions governing access to information constituting commercial, bank or other secrets by other financial institutions, as required by R.13, R.16 and R.17.

Weighting and conclusion

1396. In general, the requirements related to access by the designated financial monitoring agency to

information constituting official, commercial, bank or other secrets protected by law are met. However, there are deficiencies in the sectoral legislation of certain financial institutions related to access to such information as well as in the legislation governing exchange of information between the designated authority and other government authorities, including those responsible for overseeing compliance by financial institutions with the AML/CFT legislation within their purview, which may potentially impede access to and exchange of information. Access to information that constitutes banking secrecy and is requited for execution of international requests (if criminal proceedings are initiated outside Kazakhstan) is also restricted. The APDC is not explicitly authorized to share confidential information in the process of execution of international requests. Except for STBs, the legislation lacks any provision allowing financial institutions to share information constituting bank, commercial or other secrets protected by the law with other financial institutions, as required by R.13, R.16 and R.17.

1397. **Recommendation 9 is rated largely compliant.**

Recommendation 10 – Customer due diligence

1398. In the previous MER, Kazakhstan was rated non-compliant with former R.5. The identified deficiencies included the following: there was no direct prohibition to open anonymous accounts and accounts in fictitious names; there was no obligation to undertake the CDD measures when carrying out transactions in amount exceeding USD 15,000 and also when there is a ML suspicion; the "beneficial owner" was not defined for the AML/CFT purposes; there was no obligation to verify information obtained through the CDD process; there was no requirement to undertake enhanced CDD measures for high-risk customers; there was no requirement to perform ongoing monitoring (i.e. ongoing due diligence) of customer transactions.

1399. Besides that, the AML/CFT Law did not cover consumer credit cooperatives; pawnshops; micro credit organizations; leasing companies; insurance agents; organizations accepting from public cash as payment for the provided services received by a trustee who acts on behalf and at instructions of a trustor (service provider) under an agency contract, *inter alia*, via electronic terminals. Furthermore, the legislation did not specify frequency of updating information on the existing customers and applying the full range of CDD measures to such customers, and the CDD measures did not provide for identification and recording of information on customers that have been already served by financial institutions.

1400. **Criterion 10.1**– Opening and maintaining anonymous accounts and accounts in fictitious names is directly prohibited by the legislation. This prohibition applies to all financial institutions that open accounts or establish other similar business relationships with customers (Law 11-VI Art.27, Par.2, subpar.3; Law 461-II Art.1, Par.28; AIFC-FR0008 Section 6.6.1).

1401. At the same time, allowing unidentified persons to hold e-money (e-wallets) and perform transactions subject to threshold amounts and other conditions is offset by a ban on their redemption by the issuer and their sale to the agent (acquisition by the agent), as well as the requirement to make payments and other transactions exclusively in favour of identified e-money holders (Law 11-VI Art.44, Par.1-1, 4, 5 and 5-1).

1402. **Criterion 10.2**

a) Pursuant to Article 5, Par.2, subpar.1 of the AML/CFT Law, Section 6.2.1 of AIFC-FR0008 and the relevant ICR Requirements, FIs are required to undertake CDD measures when establishing business relationships, except for sale e-money by PSPs in amount not exceeding 100 MCI (~$762) and distribute prepaid payment cards which value does not exceed KZT 200,000 (~$450) (ICR Requirements for payment service providers).

b) Pursuant to the Article 5 Par.2, subpar.2 of the AML/CFT Law (as amended on July 1, 2022), Section 6.1.1 of AIFC-FR0008, FIs are required to undertake CDD measures when carrying out occasional transactions with the threshold not exceeding the equivalent of USD/EUR 15.000, except for some transactions (Article 5 Par.3-1 of the AML/CFT Law). However, the AML/CFT

Law does not explicitly mention the coverage of related transactions, but requires that they must be analyzed.

c) FIs are required to conduct CDD measures when carrying out occasional transactions, which are bank transfers and non-cash remittances, the amount of which exceeds 500,000 KZT (~$1,100), except for certain types of occasional transactions (Article 5 Par.3-1 of the AML/CFT Law), which constitutes a low-risk.

d) Pursuant to Article 4, Par.3 and Article 5, Par.2, subpar.2 of the AML/CFT Law, Section 6.2.2 of AIFC-FR0008 and the relevant ICR Requirements, financial institutions are required to undertake CDD measures when there is a suspicion of ML or TF, regardless of any thresholds. However, this requirement does not apply to occasional transactions that are exempt from the CDD requirements when establishing business relationship (see crit. 10.2a) (AML/CFT Law Art.5, Par.3-1, subpar.1, items 1, 2, 3 and 6).

e) Financial institutions are required to undertake CDD measures if they have doubts about the veracity of previously obtained customer identification data (AML/CFT Law Art.5, Par.2, subpar.4), but not the doubts about adequacy of obtained customer data, except for AIFC members (AIFC-FR0008 Section 6.2.2.a)

1403. **Criterion 10.3–** Pursuant to Article 5, Par.3, subpar.1, 2 and 6 of the AML/CFT Law and the relevant ICR Requirements, FIs are required to identify both permanent and occasional customers (whether natural or legal persons or foreign unincorporated entities) (AML/CFT Law Art.1, Par.4) and verify the customers' identity using reliable, independent source documents.

1404. As for other types of legal arrangements, the RK legislation does not provide for creation of unincorporated entities in Kazakhstan.

1405. The definition of "customer" includes a foreign unincorporated entity in the ICR Requirements for second-tier banks, microfinance organizations, professional securities market participants, central depository, insurance companies and stock exchange, but not for other types of financial institutions.

1406. The term "client" defined in the AIFC Regulations includes a legal person (body corporate) created under the law of a country or territory outside the AIFC (AIFC Glossary), but does not include legal arrangements.

1407. **Criterion 10.4** – Pursuant to Article 5, Par.1 of the AML/CFT Law and Section 6.3.1(a) of AIFC-FR0008, FIs are required to undertake CDD measures in respect of customers' representatives and also to verify whether such representatives are authorized to act on behalf of and/or for customers (AML/CFT Law Art.5, Par.3, subpar.6; AIFC-FR0008 Section 6.3.1(a)).

1408. **Criterion 10.5**– FIs are required to identify BOs using information and documents provided by customers or obtained from other sources (AML/CFT Law Art.5, Par.1; AIFC-FR0008 Section 6.3.1; relevant ICR Requirements) and to include the procedure of verification of veracity of BO data into the identification program.

1409. Article 5, Par.5 of the AML/CFT Law authorizes FIs to require customers to provide information and documents necessary or sufficient for identification of BOs.

1410. Pursuant to Article 5, Par.3, subpar.2-1, item 4 of the AML/CFT Law, obliged entities are required to document data necessary for identification of beneficial owners based on information and (or) documents provided by customers (their representatives) or obtained from other sources. However, the legislation does not require such other sources to be reliable.

1411. **Criterion 10.6**– Pursuant to Article 5, Par.3, subpar.4 of the AML/CFT Law, FIs are required to obtain information on the purpose and intended nature of business relationships. However, except for the AIFC members (AIFC-FR0008 Section 6.3.1, Par.(b)), FIs are not directly required by the law to understand the purpose and nature of business relationships.

1412. **Criterion 10.7**– Pursuant to Article 5, Par.1 of the AML/CFT Law and AIFC-FR0008, FIs are required to undertake CDD measures that shall include ongoing due diligence on business relationship (AML/CFT Law Art.5, Par.3, subpar.5; AIFC-FR0008 Section 6.4).

a) The CDD process includes examination of transactions carried out by customers, with obtaining and recoding information on the source of transacted funds, where necessary (AML/CFT Law Art.5, Par.3, subpar.5; AIFC-FR0008 Section 6.4.1 (a))). For most FIs, customer transaction examination frequency is determined with due consideration for the customer risk level (see the relevant IRC Requirements). However, some FIs (exchange offices, EEMA) are not explicitly requited to consider customer risk level and customer business profiles when conducting ongoing review of customer transactions. For exchange offices, this is not a deficiency, as buying, selling and exchanging foreign currency in cash is a one-off transaction.

b) FIs are required to keep documents, records or information collected under the CDD process (AML/CFT Law Art.11, Par.4; AIFC-FR0008 Section 14.5.1) and to review and update this information (AML/CFT Law Art.5, Par.3, subpar.1; AIFC-FR0008 Section 6.4.1(d)) taking into account a customer risk level (see the relevant ICR Requirements). Information on high risk customers shall be updated at least once a year (see the relevant ICR Requirements).

1413. **Criterion 10.8** – With a view to collecting information necessary for identification of legal persons and foreign unincorporated entities and identifying BOs, FIs are required to determine the ownership and control structure of customers that are legal persons and foreign unincorporated entities based on their constituent documents and registers of shareholders or other sources (AML/CFT Law Art.5, Par.3, subpar.2-1 and 2-2). FIs are also required to collect and document information about business activities of legal persons and foreign unincorporated entities (AML/CFT Law Art.5, Par.3, subpar.2 and 2-1).

1414. However, pursuant to the ICR Requirements, only some types of FIs (STBs, EEMA, securities market participants, insurance companies) are required to collect and document information on business activities and senior managers of foreign unincorporated entities.

1415. **Criterion 10.9** – For customers that are legal persons, Article 5, Par.3, subpar.2 of the AML/CFT Law requires FIs to collect and document information necessary for identification based on the state or record registration certificates and business identification numbers.

1416. According to Article 12 of Law 2198, registration certificate contains the following information:

a) Name of a legal person; information on a legal form and proof of existence of a legal person can be obtained from the "Legal Entities" database in the Register of Business Entities (Commercial Code Art.25) (The Regulation on Maintenance and Use of the Register are adopted by Government Resolution 1091 dated December 28, 2015);

b) Information on persons holding senior management positions; however, information on powers that regulate and bind a legal person is absent;

c) Location of a legal person that corresponds to the address of the registered office (Civil Code Art.39).

1417. For non-resident legal persons registered abroad, FIs are required to collect and document information necessary for identification based on the registration number of a non-resident legal person in a foreign country. However, there are no requirements for a particular form and type of a proof-of-registration document and, therefore, it is unclear what information sources should be used by financial institutions for collecting and verifying information necessary for identification of non-resident legal persons registered abroad.

1418. With a view to identifying foreign unincorporated entities, FIs are required to collect and document the following information: name; foreign registration number; location address; principle place of business; and business activities, and in case of trusts and similar arrangements, also information on assets and full

names and residential (location) addresses of settlors (members).

1419. **Criterion 10.10** – The CDD measures include identification of BOs and collection of information necessary for verification of their identity, except for a legal address, as well as verification of veracity of information necessary for identification of BOs and updating BO information (AML/CFT Law Art.5, Par.3, subpar.2-1 and 6).

1420. STBs and the central depository are permitted not to collect information about a person in favor of whom a customer carries out transactions with funds and (or) other assets, if such customer is the government authority, securities market participant or insurance company, except for the situations when there are suspicions that a customer uses business relationship for ML/TF purposes (AML/CFT Law Art.5, Par.3, subpar.2-1).

1421. **Criterion 10.11**– Pursuant to Article 5, Par.3, subpar.2-1 of the AML/CFT Law (as amended on July 1, 2022), FIs are required to collect and document information necessary for identification of foreign unincorporated entities, and are also required to identify BOs and record full names and residential (location) addresses of settlors (members) of trusts and similar arrangements.

1422. The FIs in AIFC are required to identify and verify identities of BOs of a trust, including the trustee, settlor, protector, enforcer, beneficiaries and any other persons entitled to receive a distribution (AIFC-FR0008 Section 6.3.3).

1423. The term "customer" defined in the ICR Requirements for STBs, EEMA, securities market participants, insurance companies (but not for other types of FIs) includes foreign unincorporated entities, and the requirements related to identification BOs of legal persons apply to such entities.

1424. **Criterion 10.12**–The term "customer" defined in the ICR Requirements for insurance and reinsurance companies includes a beneficiary (ICR Requirements for insurance and reinsurance companies Par.2 Subpar. 4). Therefore, it can be concluded that the CDD measures apply to beneficiaries of life insurance and other investment related insurance policies under the IRC Requirements.

a) The CDD measures include identification (identification of names) of beneficiaries that are natural or legal persons (AML/CFT Law Art.5, Par.3, subpar.1 and 2; ICR Requirements for insurance and reinsurance companies Par.23 and 24).

   When conducting CDD in respect of life insurance or other similar insurance policies, the FIs in AIFC are required to verify identities of all named beneficiaries of insurance policy (AIFC-FR0008 Section 6.3.2, subparagraph (a)).

b) The legislation does not require to obtain information concerning beneficiaries that are designated by characteristics or by class or by other means, to satisfy a FI that it will be able to establish the identity of the beneficiary at the time of the payout.

   The FIs in AIFC are required to verify the identities of persons in any class of beneficiaries, or where these are not identifiable, ensure that they obtain sufficient information to be able to verify the identities of such persons at the time of the payout (AIFC-FR0008 Par.6.3.2, subparagraph b).

c) Insurance and reinsurance companies are required to identify customers and beneficial owners before receiving insurance premiums or making insurance payouts (AML/CFT Law Art.5, Par.3, subpar.6).

   The FIs in AIFC are required to identify beneficiaries before or at the time of insurance policy payout (AIFC-FR0008 Par.6.3.2, subparagraph b).

1425. **Criterion 10.13** – The term "customer" defined in the ICR Requirements for insurance and reinsurance companies includes a beneficiary (ICR Requirements for insurance and reinsurance companies Par.2 Subpar. 4). Therefore, high-risk customers and beneficiaries are subject to enhanced CDD measures (ICR Requirements for insurance and reinsurance companies, Paras. 23, 26, 28, 29).

1426. The AIFC members are required to undertake enhanced CDD measures, which shall include reasonable measures to identify and verify the identity of the BOs of a beneficiary at the time of payout, if the beneficiary of a life insurance policy is a legal person or a legal arrangement that poses higher risk (AIFC-FR0008 Par.6.3.2).

1427. **Criterion 10.14**– Pursuant to Article 6 of the AML/CFT Law, FIs are required to identify and verify the identities of customers and BOs before establishing business relationships, and also before carrying out financial transactions with funds/and or other assets as required by the AML/CFT Law Art.7, Par.1.

1428. Except for the AIFC members, the legislation does specify that other FIs may complete verification of the identities of the customer and BO after the establishment of the business relationship, but, at the same time, does not explicitly prohibit them from doing so.

1429. Furthermore, when establishing online business relationships with customers, FIs are permitted to execute transactions, except for cross-border transactions, without taking measures for verifying veracity of information needed for identification of the customer and BO, if the customer carries out transactions involving payment of taxes, fines, penalties and other obligatory fees, insurance premiums under compulsory insurance contracts and crediting funds to customer account (AML/CFT Law Art.5, Par.3-2). However, this exemption is not substantiated as required under criterion 10.14.

1430. The AIFC members are permitted to establish business relationships before completion of verification of identity of a customer and any beneficiary owner, provided that such verification will be completed as soon as possible but not later that within 30 days after establishment of business relationship, and if this is essential not to interrupt the normal conduct of business and the ML/TF risks are effectively managed (AIFC-FR0008 Par.6.3.2, subparagraph b).

1431. **Criterion 10.15**– Except for the AIFC members, the legislation does not specify that other FIs may complete verification of the identities of the customer and beneficial owner after the establishment of the business relationship, but, at the same time, does not explicitly prohibit them from doing so (see criterion 10.14).

1432. An AIFC member is permitted to establish business relationship with a customer before completion of verification, provided that the risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification have been adopted and implemented by such company (AIFC-FR0008 Section 6.3.2).

1433. **Criterion 10.16** – FIs are required to apply CDD measures to existing customers if they have doubts about the veracity of previously obtained customer and BO data, but not in case of doubts about adequacy of such data (AML/CFT Law Article 5, Par.2, subpar.4). FIs must also update the customer data as required by the internal control rules (AML/CFT Law Article 5, Par.3, subpar.6). The customer data shall be updated based on the risk level, but at least twice a year in case of high risk customers and once in two years in case of customers posing low ML/TF risk (see the relevant ICR Requirements).

1434. **Criterion 10.17** – FIs are required to undertake enhanced CDD measures in a manner and in situations provided for in the internal control rules and also based on ML/TF risk level. Enhanced CDD measures shall be applied to customers and BOs where the risk level is high (AML/CFT Law Art5, Par.7 as amended on July 1, 2022).

1435. As part of the risk management program, FIs are required to grade their customers based on risk factors and categories. FIs are required to apply enhanced CDD measures to customers rated as posing high risk (see the relevant ICR Requirements).

1436. The FIs in AIFC are required to undertake enhanced CDD measures in respect of any customer who falls into the high risk category (AIFC-FR0008 Section 6.1.1).

1437. **Criterion 10.18**– Pursuant to Article 5, Par.1 of the AML/CFT Law (as amended on July 1, 2022), FIs are permitted to apply simplified CDD measures in a manner and in situations provided for in the

internal control rules and also based on ML/TF risk level. Simplified CDD measures may be undertaken when there is a low risk level, and are not applicable if FIs reasonably suspect that a customer establishes business relationship or carries out a transaction for the ML/TF purposes. Enhanced CDD measures are applied when there is a high risk level.

1438. Pursuant to the IRC requirements, FIs are allowed to apply simplified CDD measures to customers rated as posing low ML/TF risk. However, except for the AIFC members, the legislation contains no provisions stating that simplified CDD measures should be commensurate with the lower risk factors in each particular case.

1439. **Criterion 10.19**

a) FIs are required to refuse to perform transactions with funds or other assets for a natural or legal person or a foreign unincorporated entity and terminate business relationships when they are unable to undertake CDD measures. (AML/CFT Law Art.13, Par.1 as amended on July 1, 2022).

   The FIs in AIFC are required not to perform a transaction, not to open an account, not to otherwise establish business relationship and terminate or suspend existing business relationship with a customer when they are unable to conduct and complete the required CDD in respect of any customer (AIFC-FR0008 Section 6.6.1).

b) FIs are required to notify designated government agency of refusal to establish business relationship with a natural or legal person, termination of customer business relationship and refusal to perform a transaction with funds or other assets (AML/CFT Law Art.13, Par.2).

   The FIs in AIFC are required to consider making a suspicious transaction report when they are unable to conduct and complete the required CDD in respect of any customer (AIFC-FR0008 Section 6.6.1, Par.(f)).

1440. **Criterion 10.20** – There are no provisions in the AML/CFT Law that allow FIs, when they suspect ML/TF and reasonably believe that performing the CDD process will tip-off the customer, not to pursue the CDD process and instead file an STR. This is explained by the fact that the CDD shall necessarily be conducted in all cases, except for certain exemptions (see criterion 10.2).

1441. The FIs in AIFC are permitted not to pursue the CCD process and instead file an STR, if they reasonably believe that performing CDD will tip-off a customer or a potential customer (AIFC-FR0008, Tipping-off Guidance, Section 13.8.3, Par.(b)).

Weighting and conclusion

1442. In general, the RK legislation is largely compliant with the FATF requirements related to CDD, nevertheless there are certain deficiencies. Some low-risk occasional transactions are excluded from the requirement to implement CDD measures in case of a suspicious transaction. Some deficiencies concern possibility for FIs not to pursue the CDD process and instead file an STR.

1443. **Recommendation 10 is rated largely compliant.**

Recommendation 11 – Record keeping

1444. In the previous MER, Kazakhstan was rated largely compliant with former Recommendation 10. The identified deficiencies included the following: (i) the AML/CFT legislation requirements did not apply to leasing companies; consumer credit cooperatives; pawnshops; micro credit organizations; insurance agents; organizations accepting from public cash as payment for the provided services received by a trustee who acts on behalf and at instructions of a trustor (service provider) under an agency contract, *inter alia*, via electronic terminals (several such institutions operated in Kazakhstan); (ii) there were no clear and explicit statutory requirements to retain information on transactions with funds and (or) other assets for at least five years; (iii) there were no clear and explicit statutory requirements to retain all identification data obtained through the CDD process; and (iv) there were no clear and explicit statutory requirements to provide all

customer and transaction information at request of the competent authorities in a timely manner.

1445. **Criterion 11.1**– FIs are required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction (AML/CFT Law Art.11, Par.4 as amended on July 1, 2022).

1446. The sectoral legislation (Law on Commodity Exchanges Art.22, Par.2; Law 11-VI Art.12, Par.12) requires some FIs to keep records of performed transactions and retain this information for five years following completion of a transaction. Similar requirements are also set out in the AIFC Regulations for FIs (AIFC-FR0008 Section 14.5.1).

1447. **Criterion 11.2** – FIs are required to keep all records obtained through CDD measures, including customer files, customer data and business correspondence, for least five years following termination of business relationship (AML/CFT Law Art.11, Par.4).

1448. FIs are required to retain documents and records of transactions with funds or other assets that are subject to financial monitoring and suspicious transactions as well as results of analysis of all complex, exceptionally large and other unusual transactions for at least five years following completion of a transaction ((AML/CFT Law Art.11, Par.4). Similar obligations are set out in the ICR Requirements for all FIs.

1449. The FIs in AIFC are required to keep supporting records related to customer business relationships and transactions for at least six years following submission of a notification or report, termination of business relationship or completion of transaction, whichever occurs later (AIFC-FR0008 Section 14.5.1).

1450. **Criterion 11.3** – Documents and records shall be sufficient to permit reconstruction of individual customer transactions, including transaction currency and amount (AML/CFT Law Art.11, Par.4), so as to provide evidence for criminal investigations and prosecutions as required by Articles 111, 112, 118, 120 and 122 of the RK Criminal Procedure Code.

1451. **Criterion 11.4** – FIs are required to report transactions that are subject to financial monitoring to the FIU and to the government authorities responsible for supervising compliance by FIs with the AML/CFT legislation within their purview (AML/CFT Law Art.10, Par.2; Law 474-II Art.14; Presidential Decree 1271 Par.17; Presidential Decree 428 Par.16). However, there are shortcomings in accessing information by other competent authorities, as indicated in R.9.

Weighting and conclusion

1452. In general, the legislation is compliant with Recommendation 11. However, direct access to information by the government authorities other than FIU and supervisors is limited.

1453. **Recommendation 11 is rated largely compliant.**

Recommendation 12 – Politically exposed persons

1454. In the previous MER, Kazakhstan was rated partially compliant with former Recommendation 6. The identified deficiencies included the following: (i) the AML/CFT requirements did not apply to consumer credit cooperatives; pawnshops; microcredit organizations; leasing companies; insurance agents; organizations accepting from public cash as payment for the provided services received by a trustee who acts on behalf and at instructions of a trustor (service provider) under an agency contract, *inter alia*, via electronic terminals; (ii) no identification of existing customers was performed for recording information on them as well as for determining whether they are politically exposed persons; (iii) measures for enhanced ongoing monitoring of the relationships with PEPs were not developed; and (iv) no timelines were established for regular verification of customer information to identify PEPs.

1455. **Criterion 12.1**– In relation to foreign PEPs, in addition to performing the CDD measures, FIs are required to take additional measures (AML/CFT Law Art.8; AIFC-FR0008 Section 5.1.4; the relevant IRC Requirements). In particular, FIs are required to:

a) Determine whether a customer and BO is a foreign PEP (AML/CFT Law Art.8, Par.1, subpar.1). The customer and BO identification program shall include description of measures aimed at identification of foreign PEPs among existing and newly on-boarded customers and beneficial owners (ICR Requirements for second-tier banks Par.22; ICR Requirements for single pension savings fund Par.25; ICR Requirements for non-financial sector entities Par.24; ICR Requirements for exchange offices Par.27; ICR Requirements for microfinance organizations Par.25; ICR Requirements for payment service providers Par.27; ICR Requirements for postal operators Par.27; ICR Requirements for professional securities market participants Par.29; ICR Requirements for insurance companies Par.26; ICR Requirements for commodity exchanges Par.27; ICR Requirements for stock exchange Par.26; ICR Requirements for AIFC Par.22).

b) Obtain approval of the senior manager of an institution before establishing and continuing business relationships with customers who are foreign PEPs (AML/CFT Law Art.8, Par.1, subpar.3; AIFC-FR0008 Sections 6.3.3 and 6.3.4).

c) Take available measures to establish the source of funds of customers and BOs (AML/CFT Law Art.8, Par.1, subpar.4).

   The FIs in AIFC are also required to understand the source of wealth of customers (AIFC-FR0008, Section 6.3.1, Par.(c) and (d)). Thus, FIs, except for the AIFC members, are not required to establish the source of wealth of customers and BOs.

d) Conduct enhanced due diligence in respect of customers and BOs (AML/CFT Law Art.8, Par.1, subpar.5), which, however, does not include enhanced ongoing monitoring of that relationships.

1456. The above measures are not applied to foreign PEPs who no longer discharge their functions.

1457. **Criterion 12.2** – In addition to performing the CDD measures, FIs are also required to take additional measures in respect of domestic PEPs who are included in the list of public officials (adopted by the RK President) identified as posing high risk (AML/CFT Law Art.8, Par.2).

1458. Persons holding senior management positions in international organizations are covered by the definition of PEP (AML/CFT Law Art.1, Par.3-1) and, therefore, additional measures mentioned in criterion 12.1 apply to them. However, these measures are not applied to PEPs who no longer discharge their functions in international organizations.

1459. Pursuant to the IRC Requirements for STB, when identifying existing or newly on-boarded customer and BO, STBs are required to determine whether such customer and BO are domestic PEPs (ICR Requirements for second-tier banks Par.26).

1460. In relation to PEPs included in the list of public officials (adopted by the RK President) identified as posing high risk, FIs are required to apply the same additional measures as those applicable to foreign PEPs (AML/CFT Law Art.8, Par.2).

1461. **Criterion 12.3** – Except for the FIs in AIFC (AIFC Glossary), the requirements of criteria 12.1 and 12.2 apply to spouses and close family members of PEPs (AML/CFT Law Art.8, Par.1 and 2), but do not apply to close associates of PEPs. See analysis of criteria 12.1 and 12.1 и 12.2.

1462. **Criterion 12.4** – According to the ICR Requirements for insurance and reinsurance companies, the term of "customer" includes the beneficiary (ICR for insurance and reinsurance companies, Para.4, Subpara.2). Thus, CDD measures, including the identification of the BO, apply to beneficiaries of life and other investment-related insurance policies. The measures are applied prior the insurance payment (see Cr. 10.12, 10.13). The FIs in respect of PEPs are additionally required to verify the affiliation and/or relationship of the customer (beneficiary) and the BO with the PEP, his/her close relatives, and to obtain written approval from the FI's management for the establishment, continuation of business relations with such customers.

1463. The FIs in AIFC are required to take reasonable measures to determine whether the beneficiaries of

life insurance policy or the BO of the beneficiary are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, the FIs in AIFC are required to inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report (AIFC-FR0008 Section 6.3.2).

Weighting and conclusion

1464. The legislation contains the PEP-related provisions that are, to a large extent, consistent with the FATF Standards. However, there are some deficiencies related to domestic and foreign PEPs, additional measures do not apply to foreign PEPs and PEPs of international organisations who have ceased to perform their functions, and there is no requirement to conduct enhanced ongoing monitoring of business relationships with PEPs. There are no specific requirements for applying additional measures in relation to PEP's associates.

1465. **Recommendation 12 is rated largely compliant.**

Recommendation 13 – Correspondent banking

1466. In the previous MER, Kazakhstan was rated partially compliant with former Recommendation 7 due to the following deficiencies: (i) there were no requirements for gathering sufficient information on a respondent institution to fully understand the nature of its business and whether it had been subject to AML/CFT sanctions; (ii) there were no requirements to assess the respondent institution's AML/CFT controls; and (iii) financial institutions were not required to document the AML/CFT responsibilities of each institution.

1467. **Criterion 13.1**– Establishment of correspondent relationships by STBs and EECTBOs is regulated by the AML/CFT Law, while establishment of correspondent relationships by the FIs in AIFC is regulated by AIFC-FR0008. However, AIFC-FR0008 and the AML/CFT Law do not apply to establishment of other similar relationships as required by the Standard.

a) When establishing correspondent relationships with FIs, STBs, branches of non-resident banks and EECTBOs are required to gather, from publicly accessible sources, and document information about reputation of a foreign respondent institution and nature of its business, including whether it has been subject to investigation and sanctions for breaches of its home country's AML/CFT legislation (AML/CFT Law Art.9, Par.1). This is more limited compared to the FATF Standards that require FIs to verify whether a respondent institution has been subject regulatory action and not just sanctioned for breaches of the legislation.

   The legislation does not require all FIs to gather sufficient information about a respondent institution to determine the quality of supervision of the respondent institution.

   When establishing correspondent banking relationship with a respondent bank, the AIFC members are required to gather sufficient information about the respondent bank to understand fully the nature of the respondent bank's business, and to determine from publicly available sources the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action. (AIFC-FR0008, Section 10.2.1, Par.(a), (b) and (c)).

b) FIs are required to assess the effectiveness of AML/CFT internal controls implemented by a respondent institution (AML/CFT Law Art.9, Par.2; AIFC-FR0008, Section 10.2.1, Par.(d)).

c) FIs are required to obtain approval from a senior manager for establishing new correspondent relationships (AML/CFT Law Art.9, Par.3; AIFC-FR0008, Section 10.2.1, Par.(e)).

d) STBs, branches of non-resident banks and EECTBOs are not explicitly required to clearly understand the division of AML/CFT responsibilities between correspondent institutions. However, pursuant to paragraph 7 of NB Board Resolution on Approval of Rules and Procedures

of Establishment of Correspondent Relationships No.210 dated August 31, 2016, correspondent institution may open a correspondent account for a respondent institution only after undertaking CDD measures in respect of the respondent's customers and BOs as required by the AML/CFT Law.

The FIs in AIFC are required to understand the division of responsibilities among correspondent relationship parties and ascertain that the relevant responsibilities of the parties are properly documented (AIFC-FR0008, Section 10.2.1, Par.(f)).

1468. **Criterion 13.2** – With respect to "payable-through accounts", FIs should be required to satisfy themselves that the respondent institution:

a) has performed CDD obligations on its customers that have direct access to the accounts of the correspondent bank (AML/CFT Law Art.9, Par. 2-1; AIFC-FR0008, Section 10.2.1, Par.(g)); and

b) is able to provide relevant CDD information upon request to the correspondent bank (AML/CFT Law Art.9, Par. 2-1; AIFC-FR0008, Section 10.2.1, Par.(g)).

1469. **Criterion 13.3** – FIs are prohibited from entering into, or continuing, correspondent relationships with shell banks (AML/CFT Law Art.9, Par.3; AIFC-FR0008, Section 10.2.1, Par.4(ii)), and are required to satisfy themselves that respondent institution does not permit its accounts to be used by shell banks (AML/CFT Law Art.9, Par.4; AIFC-FR0008 Section 10.2.1, Par.4(ii)).

Weighting and conclusion

1470. The legislation, as is pertains to establishing and maintaining correspondent relationships, is generally compliant with the Recommendation13 with minor deficiencies related to absence of the requirement concerning other similar relationships.

1471. **Recommendation 13 is rated largely compliant.**

Recommendation 14 – Money or value transfer services

1472. In the previous MER, Kazakhstan was rated non-compliant with former Special Recommendation VI, as (i) a portion of the MVTS operators were not licensed; and (ii) the established requirements did not apply to some MVTS operators. There were also some deficiencies related to the AML/CFT measures in the banking sector applicable to banks in context of money remittances.

1473. **Criterion 14.1**– In Kazakhstan, money or value transfer services (MVTS) are provided by:

- The National Bank, STBs, EECTBOs, postal operators, PSPs (Law 11-VI Art.10, Par.1, subpar.1-5), payment agents and sub-agents (Law 11-VI Art.10, Par.1, subpar.6-7), and
- The AIFC members that provide payment services (AIFC General Rules, Section 3, Par.20 and 26).

1474. However, the NB acts as a technical operator to ensure the operation of the national payment system. The NB only opens and maintains correspondent accounts for STBs in national and foreign currencies. Money transfer systems are not authorised to provide payment services in Kazakhstan. These systems organise processing, message routing, authorisation and clearing.

1475. Provision of payment services without obtaining a license from the ARDFM or without record registration with the NB is prohibited in Kazakhstan (Law 11-VI Art.13, Par.1). However, payment agents and sub-agents of payment system are not required to be licensed or registered under the legislation (Law 11-VI Art.13, Par.1, subpar.2).

1476. Postal services include, among other things, postal money transfer services (Law 498-V Art.9, Par.2, subpar.4), banking services and financial transactions provided for in the legislation (Law 498-V Art.9, Par.3, subpar.1). The national postal operator is authorized to carry out certain types of banking

transactions, including payment and money transfer transactions for natural and legal persons, without license (Law 498-V Art.23, Par.2, subpar.3).

1477. The AIFC General Rules stipulate that the activities of any AIFC member, including the MVTS provider, shall be licensed (sub-paragraph 1.1.1 (a) of paragraph 1).

1478. **Criterion 14.2**– Provision of payment services without obtaining a license from the ARDFM or without record registration with the NB is prohibited in Kazakhstan (Law 11-VI Art.13, Par.1).

1479. Banking transactions carried out without license issued by the designated government authority or the National Bank are invalid (Law 2444 Art.6, Par.2).

1480. Business and banking activities (including banking transactions) carried out without registration and/or license or in breach of the RK legislation on permits and notifications entail:

- Criminal liability under Criminal Code Article 214 which are punishable by: fine in amount of up to 2,000 MCI (~USD 13,600), or correctional work or community services for up to 600 hours, or restriction of liberty or imprisonment for up to 2 years with or without confiscation of property; if committed repeatedly or by a group of persons, these actions are punishable by: fine in amount of up to 5,000 MCI (~USD 34,000), or correctional work or community services for up to 1,200 hours, or restriction of liberty or imprisonment for up to 5 years with confiscation of property;
- Administrative liability under Code of Administrative Offences Article 155 which are punishable by fine in amount from 30 MCI (~USD 204) to 50% of inflicted losses or derived illegal proceeds imposed depending on the subject of the offence (natural person) and the size of the MVTS provider (small, medium, large businesses); under Article 463 - fine in amount from 15 MCI (~USD 102) to 150 MCI (~USD 1,020) depending on the subject of the offence (natural person) and the size of the MVTS provider) with or without confiscation of administrative offence instrumentalities, proceeds (dividends), money and securities obtained through administrative offence; if committed repeatedly during one year after imposition of administrative sanctions, these actions are punishable by fine in amount from 30 MCI (~USD 204) to 500 MCI (~USD 3,400) with confiscation.

1481. There are no regulatory prescriptions for KazPost to identify individuals and legal persons providing MVTS without a licence or registration.

1482. In relation to MVTS in AIFC, upon detection of breaches of the AIFC regulations, the AFSA may impose the following sanctions: impose a fine; issue a reprimand; require an offender to pay restitution or compensation of affected person; order an offender to provide a report on illegal proceeds or enrichment as a result of committed offences; order an offender to cease the activity constituting the offence; require an offender to remedy the committed breaches; prohibit an offender from holding position or being employee of the authorized person (FSFR Section 118).

1483. Pursuant to FSFR Section 127, at request of the AFSA, the AIFC Court may order to compensate inflicted losses, if it is proved that a person has committed a breach within the meaning of Section 127, including prohibition from carrying out activities without license, as a result of which the offender derived a benefit or other persons suffered losses.

1484. When imposing a penalty (fine or other corrective measure), the AFSA shall proceed from the seriousness of the violation committed, the existence of intent, an assessment of the consequences of the act committed (FSFR Section 129).

1485. Operation in the capacity of MVTS provider without a license in the AIFC territory, if it constitutes a criminal offence, is punishable under the RK criminal legislation. Criminal liability for unlicensed or illegal activity is imposed under Article 214 of the Criminal Code.

1486. **Criterion 14.3** – STBs, branches of non-resident banks, EECTBO, postal operators, PSPs are obliged entities (Article 3 of the AML/CFT Law) and are subject to all the requirements of the AML/CFT Law.

International money transfer services are not obliged entities, however they only operate through STBs and are subject to AML/CFT requirements.

1487. Activities of the AIFC members related to provision of payment services and management of payment systems are considered to be financial services and, therefore, are subject to financial monitoring under AIFC-FR0008.

1488. **Criterion 14.4** –STBs, EECTBOs and PSPs are permitted to provide payment services through payment agents and sub-agents under the agency agreements. Payment agents and sub-agents are not subject to licensing or registration (Law 11-VI Art.13, Par.1, subpar.2). However, STBs, EECTBOs and PSPs are required to maintain registers of their payment agents and sub-agents as provided for in the agency agreements and internal regulations (Law 11-VI Art.14).

1489. No information has been provided as to whether or not KazPost is permitted to provide services through payment agents and sub-agents.

1490. Operation of persons in the capacity of agents or sub-agents, unless they are incorporated or registered as AIFC members, is prohibited (AIFC-2-2017, Section 7, Par.1).

1491. **Criterion 14.5** – MVTS providers that use agents (sub-agents) are required to include them in their AML/CFT programs developed in line with the AML/CFT Law and monitor them for compliance with these programs (ICR Requirements for payment service providers, Par.4, subpar.3).

Weighting and conclusion

1492. The licensing or registration requirements apply to all categories of MVTS providers, except for payment agents and subagents. The KazPOst is exempt from these requirements as it is permitted to carry out certain types of banking transactions without a license. The National Bank, being the government authority, provides payment services, and it is not the obliged entity as per the AML/CFT Law.

1493. **Recommendation 14 is rated largely compliant.**

Recommendation 15 – New Technologies

1494. In the last MER, the Republic of Kazakhstan achieved the "Non-compliant" rating under previous Recommendation 8 due to the following: i) FIs are not obliged to develop or apply special procedures for preventing the misuse of technological developments for ML/TF purposes; ii) FIs are not obliged to develop procedures for managing the risks associated with non-face to face business relationships and transactions.

New Technologies

1495. **Criterion 15.1** – At the national level, assessment of risks of technological developments use is prescribed by Article 11-1 of the AML/CFT Law and obliged entities must perform this assessment of risks (Sub-par. 1) of Par. 6) at the time of evaluation, identification, documentation and update of ML/TF risks assessment results.

1496. Moreover, obliged entities must develop, among other things, a program for internal control associated with ML/TF risks management that would factor in the risk of using services for criminal purposes, including the risk of using technological developments (Paragraph 3 of Par. 3 of Article 11 of the AML/CFT Law). This requirement is made more specific in regulations of the majority of obliged entities categories prescribing that ML/TF risks should be identified both for new and for existing products:

- Chapter 3 (Par. 26) of ICR Requirements for gambling industry and lotteries;
- Chapter 3 (Par. 23) of ICR Requirements for non-financial sector;
- Chapter 3 (Par. 24) of ICR Requirements for notary officers;
- Par. 19-1 of ICR Requirements for entities engaged in certain types of banking operations, microlenders;

- Chapter 3 (Par. 26) of ICR Requirements for post operators providing money transfer services;
- Par. 22-1 of ICR Requirements for Securities Market participants;
- Par. 20-1 of ICR Requirements for STB and National Post Operator;
- Par. 21-1 of ICR Requirements for insurance companies;
- Chapter 3 (Par. 26) of ICR Requirements for commodity exchange;
- Chapter 3 (Par. 13, Subpar. 7) of ICR Requirements for payment service providers;
- Chapter 3 (Par. 23) of ICR Requirements for persons in the area of virtual assets;
- Sub-par. 4.1.3 of AIFC-FR0008 to be applied by all categories of AIFC members.

1497. There is no requirement to identify and assess ML/TF risks specifically related to new services (products) in the ICR for AIs (exchange offices) due to the specific nature of their activities (cash exchange only), which is a deficiency, given the importance of the sector and the ML/TF risk of using cash as identified by the NRA.

1498. **Criterion 15.2**

a) Statutory requirement that ML/TF risks should be assessed prior to launching new products, business practice or use of new or emerging technologies is set in ICR Requirements for all FIs (except for AIs) and DNFBPs and AIFC members, as mentioned in Criterion 15.1;

b) As part of their ICR, obliged entities must apply controls and procedures for ML/TF risks management and mitigation (Part 2 of Par. 3-1 of Article 11 of the AML/CFT Law).

This general statutory provision for control and mitigation of the identified ML/TF risks associated with the use of new emerging technologies is detailed in the ICR requirements of financial monitoring entities demonstrated during the on-site mission, including the ICR of payment service providers and exchange offices.

The obliged entities in AIFC are required to identify, assess the risks, mitigate and manage them (Sub-par. 4.1 of Par. 4 of AIFC-FR0008). In particular, obliged entities must use the information obtained as a result of business projects evaluation so as to ensure that their policy, controls and procedures adequately mitigate the risks identified (Sub-par. 4.2.2 (b) of Par. 4 of AIFC-FR0008). Risk management procedure is to be updated and revised on a regular basis (Par. (g) of Guidance on the Risk-Based Approach AIFC-FR0008). These regulations are detailed in Par. 3.10 of the AFSA Practical Guidance on AML/CFT.

Virtual Assets and Virtual Asset Service Providers

1499. Transactions in virtual assets are permitted in the Republic of Kazakhstan. The peculiarity of such transactions is that they are performed in AIFC where a special operation treatment has been developed, as well as in other areas of the country which are subject to the national laws. Only secured assets can be issued in the Republic of Kazakhstan (Par. 2-3 of Article 33-1 of RK Law -418-V). Both secured and unsecured assets can be issued in AIFC. Transactions in virtual assets are subject to the AML/CFT Law. However, it is worth noting the legal framework for VASPs outside the AIFC was in its formative stage as of on-site mission (there were three regulations in place).

1500. There are 8 VASPs registered in AIFC, 6 of which have medium risk level (1 cryptocurrency broker and 5 crypto-exchanges) and 2 have high risk level (1 crypto-exchange and 1 tokenised securities exchange). As of on-site mission, there were no VASPs outside the AIFC.

1501. According to the laws of the Republic of Kazakhstan and the AIFC laws (Article 115 of CC, Article 1, subpara. 55-1) of Article 1 of Law 418-V, the Glossary of AIFC), the “virtual asset” term shall cover the “transactions in money and/or other assets” term of the AML/CFT Law.

1502. **Criterion 15.3**

a) In accordance with Par. 2.1 of the Roadmap for Development of Crypto-Industry and Blockchain Technologies in the Republic of Kazakhstan, which was approved on 05/10/2021 by the MDD jointly with AIFC, ARDFM, NB, FMA (Working Group), the assessment of ML/TF risks of virtual assets has been conducted. The report was approved on 24.12.2021 by the Director General of AIFC and was submitted to the Working Group by letter AFSA-G-EC-2021-0052 dated on 24.12.2021.

   The report analyzes the risks associated with the use of specific services with digital assets in AIFC through crypto-exchanges for ML/TF purposes. This includes a vulnerability study on the adequacy of AML/CFT measures in AIFC and not in the country. Based on the results of the analysis and the VA risk assessment, the ML risks are medium; the TF risks are medium; the risk of AIFC involvement in ML and TF schemes is medium.

   In addition, the AFSA conducted ML/TF risk assessment of the sector of FinTech, including VASPs, in 2021. As part of this assessment, AFSA identified the residual risks of VASPs in AIFC at the first stage, and then analyzed the vulnerabilities to ML/TF risks taking into account the NRA, and determined the sector's rating. As a result of sectoral assessment, the ML/TF risks are medium.

   No such assessment has been carried out for those involved in issuing and trading digital assets and providing services for the exchange of digital assets for money, value and other assets, as there are no VASPs in the country;

b) Analysis of risks associated with the use of digital assets in AIFC provides for risk mitigation measures both in relation to the use of VA and in relation to the activities of VASPs: improving internal control procedures, strengthening rules for settlement using VA, strengthening interaction with the regulator, implementing cyber-, IT-security procedures. This analysis contains a list of signs/criteria for suspicious transactions with VA and VASPs. However, the risk mitigation measures do not include regulatory changes, despite the fact that the legal framework for VAPSs outside the AIFC is in its formative stage, as stated in para 1498.

   In addition, AFSA is guided by a policy document for 2021-2022 – Action Plan dated 22.08.2021 No. AFSA-B-MC-2021-0057 on Financial Crime Risk Management, containing a set of measures to reduce financial crime risks, which includes sections on inter-agency cooperation, standard setting, supervision, capacity building, awareness raising. There are no such policies for VASPs outside the AIFC.

   AFSA and MDD seniors work in inter-agency commissions, panels, high-level councils, and participate in the development of other policy documents that seek to regulate the sector to mitigate risks;

c) VASP in AIFC and VASP outside AIFC are subjects of the AML/CFT Law (Sub-par. 19) and Sub-par. 20) of Par. 1 of Article 3), and they are fully covered by the requirements for identification, assessment, control and taking efficient measures for mitigation of ML and TF risks (Articles 11 and 11-1 of the AML/CFT Law). In addition, there is the AIFC-FR0008 for VASPs in AIFC, and MDD has developed IRC Requirements for VASPs outside of AIFC. These documents detail certain provisions of the Act in relation to the mitigation of own risks.

   For example, the IRC require all relevant risk factors to be considered before determining the overall level of risk for ML/TF risk management purposes. The VASPs outside AIFC should develop an ML/TF risk management programme that considers customer risks and the risks of the use of services for criminal purposes, including the risk of the use of technological advances (Chapter 3). The obligation to update the results of the risk assessments is set out in sub-para. 1 of Article 11-1(6) of the AML/CFT Law. With regard to ML/TF risk mitigation, the CDD Requirements provide for the development and approval of the CDD, introduction of amendments and/or additions to them by the head of the obliged entities, as well as monitoring of implementation and compliance with the CDD (clause 11(1) of the CDD Requirements). The results of the ML/TF risk assessment shall be made available at the request of the relevant state authorities and non-profit organizations, of

which the VASPs outside AIFC are members (part 5 par 16 of Chapter 3 of the Requirements to the AML/CFT).

VASPs in AIFC are guided both by the above provisions of the AML/CFT Law and by AIFC law when assessing and mitigating ML/TF risks. In particular, Chapter 4 of AIFC-FR0008 requires VASPs in AIFC to apply risk-based approach, to assess business and client risks of AIFC members, availability of internal policies, procedures, systems and controls. RBA Guidance of AIFC-FR0008 and Sub-par. 1 of Par. 6 of Article 11-1 of the AML/CFT Law prescribes regular revision of the risk management process for AML/CFT purposes.

Pursuant to paragraph 13.3.1 of the AIFC AML/CFT Rules, the responsible AML/CFT officer of the obliged entity shall, at the request of the AFSA, provide any requested information.

Also, according to the AML/CFT Law, entities must disclose information on ML/TF risks identification analysis and monitoring of organizations and individuals to the FMA according to the procedure and within the time limits established by FMA (Sub-par. 13-8) Par. 1 of Article 16 of the AML/CFT Law).

1503. **Criterion 15.4**

a)

VASP (individual or legal person) cannot perform such activities, unless it holds a license from the AFSA, has not passed through state registration or has not been registered as AIFC member (Par. 24 of AIFC Framework Regulations).

There are no requirements on licensing the VASPs outside AIFC. Should the VASP outside AIFC is an individual, it must notify the MDD of the commencement or completion of activities (Par. 10 of Article 31-1 of RK Law -418-V) as well as the FMA of the commencement or completion of activities as an obliged entity. If the VASP is a legal person, it must be registered in Kazakhstan and notify the FMA respectively. As of the on-site mission there were no VASPs outside AIFC;

b) requirements for applicants, officials or persons involved in activities of a AIFC member are stated in AIFC General Rules No. FR0001 2017:

- When obtaining a license for managing the virtual assets trading platform system: i) with regard to applicants for managing the company's affairs, their relation to market abuse, financial crime or money laundering will be studied (1.2.3(d) of the General Rules); ii) with regard to the members of the company's governing body, any matter which may harm or may have harmed the integrity or the reputation of the AIFC or AFSA, including through the carrying on of a business by the applicant for a purpose connected with market abuse or a financial crime will be studied (1.2.5(h) of the General Rules);
- When applying to AIFC for a license (registration), the applicant will be subject to a comprehensive review of circumstances which may harm or may have harmed the integrity or the reputation of the AFSA or AIFC, including through the carrying on of a business by the applicant for a purpose connected with a Financial Crime (1.1.5(i), 1.2.5 of the said General Rules);
- AFSA shall review the competency of the appointed officials (executive director, financial director, compliance officer, AML/CFT specialist) at the time of appointment.

1504. AFSA shall identify VAPSs' BOs of at least 10 %, take measures for identification and understanding the legal ownership and control of a corporate customer and identification of the BO subject to the risk level of the company and the source of funds (Article 14-1, Article 179-1 of the AIFC *On Companies*, Par. 6.4.3 (c) of the AIFC AML/CFT Rules), as well as to check VASPs' BOs on active (unexpunged and unexpunged) criminal record (paras.1.3 and 4.3(a) of the Regulatory Guidance On Fitness and Propriety). VASPs are required to check active criminal records of their officials (para. 5.16 of the Regulatory

Guidance).

1505. The managers of VASPs outside AIFC and an employee responsible for AML/CFT compliance must have impeccable business reputation and no record of unquashed or outstanding conviction (for economic crimes or intentional crimes of average gravity, grave and especially grave crimes) (Part 4 of Par. 10 of ICR Requirements for virtual asset organizations). VASPs outside AIFC are required to identify BOs in accordance with national legislation (see R.24). There are no requirements in the laws of the Republic of Kazakhstan for singling out any persons with criminal record out of BOs or affiliates thereof.

1506. **Criterion 15.5** VASP in AIFC cannot do business unless they are registered by the state or registered as AIFC members (Par. 7 of AIFC-2-2017). Being authorized to perform inspections and supervision, AFSA in cooperation with LEA shall identify AIFC members that carry out activities without registration or license. AFSA imposes sanctions thereon (Par. 7 of Chapter 1, p. 8-9, Par. 118 of AIFC Framework Regulations), also for failure to comply with the AIFC prohibitions and requirements. The AFSA has a a varied types of sanctions and corrective measures and can impose the following types of punishment (one or more): a penalty (to an amount the AFSA thinks fit), conviction for violation, payment of compensation, requesting for a report on unfounded enrichment or profit; termination or suspension of VASP business, instruction to rectify a violation, prohibition on holding offices or jobs at any AIFC organization. The AFSA can exercise any other powers in accordance with the applicable laws.

1507. Subject to Par. 127 of FSFR, upon application of AFSA, the AIFC court shall be entitled to issue a ruling/award on indemnification in case it is proved that the person committed a violation under Par. 119, including an infringement of the AIFC's right (in this case, violation of Par. 24 FSFR on prohibition on unlicensed activities) that resulted in benefit for the violating person or losses for person(s).

1508. Criminal liability is provided for failure to comply with the notification procedure (Article 214 of the CC), This is applicable to VASPs both in and outside of AIFC. Also, there is an administrative liability under Article 463 of the CAO for VASPs outside the AIFC engaged in secured digital asset turnover activities without a notification (see R.35). In 2020-2021, 37 illegal VASPs were identified and their activities were terminated, and MDD and AFSA hold joint meetings on blocking the websites of illegeal VASPs (see para 891).

1509. **Criterion 15.6**

a) AFSA performs AML/CFT monitoring and control over activities of VASPs in AIFC. The AFSA has broad powers on regulation, control and supervision over VASPs, develops and adopts draft AIFC acts on the issues that fall within the scope of financial services regulation (Par. 3 of Article 12 of the Constitutional Law, Par. 7 (3) (a) of AIFC Financial Services Framework Regulations, AIFC Regulations No. 18 dated 2017).

   According to para. 1.2 of Supervisory Powers Guidance, AFSA shall apply risk-based approach to regulation and supervision over obliged entities in AIFC. For the purpose of identification, assessment, minimization and control of these risks, AFSA liaise with obliged entities and FMA.

   In addition, in accordance with the para. 1.3 of this Guidance, the risk-based approach of the AFSA to supervision of VASPs varies according to the size, scope, nature and circumstances of each particular obliged entity and specific risks posed by obliged entities in terms of regulation and supervision.

   The nature and rate of interaction between AFSA and VASPs depend on the level of the VASP exposure and many other factors (the para. 1.6 of the Guidance).

   The Ministry of Digital Development, Innovation and Aerospace Industry shall perform AML/CFT regulation and control over activities of VASP outside AIFC. This Ministry develops ICR requirements and other methodical documents for this controlled category of obliged entities. Given that countering ML/TF is covered by state control and supervision (Par. 57) of Article 138 of the COMC), inspections and supervisory actions with regard to VASP outside AIFC must be performed

according to the COMC. The COMC defines a risk assessment system as the main element of state control and supervision (Article 141). However, the result of the ML/TF risks assessment is ignored at the time of selection of entities to be inspected.

b) Subject to Par. 95 of AIFC Financial Services Framework Regulations, the AFSA can exercise any supervisory powers with regard to VASP if thinks it necessary or desirable according to its control and supervisory functions. It is authorized to collect any information, to report on any matter, to enter premises of VASP for the purpose of inspection, as well as to take copies of and study the stored information (Par. 96 to 97 of AIFC Framework Regulations). The AFSA can limit validity of a license, revoke or suspend licenses of VASP (Par. 98 of AIFC Framework Regulations), impose prohibitions on activities of VASP (Par. 99) and lay down certain requirements (Par. 100), as well as to apply punishments for violations in the form of penalties, convictions, instructions to pay compensations, suspension of business, etc. (Par. 118).

   The members shall annually submit to AFSA a report on AML/CFT (Sub-par. 13.7 of Par. 13 of AIFC-FR0008 as amended on December 12, 2021).

   Subject to Article 137 of the EC, control and supervision over activities of subjects (objects) of control and supervision shall take forms of inspection and preventive control and supervision of precautionary and preventive nature. Preventive control and supervision shall be divided into preventive control and supervision with visit to the subject of control and supervision and preventive control and supervision without visiting the subject of control and supervision. Inspection, preventive control and supervision with visit to the subject of control and supervision shall involve a visit to the subject, requesting the required information, summoning the subject of inspection (Article 140 of the EC). In view of the absence of a requirement to be licensed , no revocation, suspension, cancellation of the license can be applied against the VASPs outside AIFC. Sanctions against VASP outside AIFC can take the forms of criminal, administrative, disciplinary and other liability, as in case of other obliged entities categories, officials cannot be held administratively liable if the VASP is a state or quasi-state organisation (see R. 35). The Ministry of Digital Development, Innovation and Aerospace Industry is not authorized to apply punishments. In the absence of a requirement for licensing or registration, VASP outside AIFC cannot be subjected to license revocation, suspension or cancellation.

1510. **Criterion 15.7**– The AFSA in coordination with FMA establishes ICR Requirements for AML/CFT purposes with regard to obliged entities in AIFC (Par. 3-2 of Article 11 of the AML/CFT Law).

1511. According to AIFC-FR0008, ICR shall include policies, procedures and systems for AIFC obliged entities control, including the relevant programs for AML/CFT training and awareness raising among employees (Par. 4.3.1 of the Rules). Par. 14 of AIFC-FR0008 contains requirements and guidance on AML/CFT training and awareness raising among employees using a risk-based approach.

1512. For VASP outside AIFC, ICR Requirements have been developed and approved by joint Order No. 20 of the FMA Chairman dated February 28, 2022 and Order No. 68/nk of the Minister of the Ministry of Digital Development, Innovation and Aerospace Industry dated February 28, 2022. Acquiring of knowledge and skills for implementing AML/CFT laws is a requirement of the program for AML/CFT education and training of employees for VASP outside AIFC (Chapter 6 of the ICR Requirements). The training program shall include: i) employees training procedure including training theme, methods, time limits and business unit (person) responsible for training; ii) list of obliged entities business units (employees) to be trained; iii) procedure and forms of training results retention; iv) procedure and forms of assessing employees' knowledge of AML/CFT issues.

1513. The Ministry of Digital Development, Innovation and Aerospace Industry has developed ML/TF countering recommendations for entities involved in issuance of virtual assets and arranging trading therein and providing services for exchanging virtual assets for money, things of value and other property, as well as the Rules for Applying Risk-Based Approach to Mitigating Money Laundering and Terrorism Financing

Risks Associated with Turnover of Secured Virtual Assets, as approved by Order No. 22/NK dated September 15, 2022.

1514. FMA posts outreach information on its website (https://www.gov.kz/memleket/entities/afm?lang=ru) for all obliged entities categories, including VASP. For example, the website contains a typology of ML involving cryptocurrencies, the List of States (Areas) that Fail to Observe the FATF Recommendations, reminders to financial monitoring entities, useful links for obliged entities ; "Question–Answer" and "Contact us" sections have been actively used. See IO.3 for information on operation of the "Personal Account" online service at the FMA portal on the Internet.

1515. The FMA provides clarifications about application of AML/CFT legal norms via Telegram FMA Channel (around 6 thousand subscribers).

1516. The AFSA and MDD have mechanisms for interaction with the VASPs on AML/CFT, however, such interaction is less likely to involve feedback to the VASPs. Feedback is mainly provided by the FMA.

1517. **Criterion 15.8**

a) As an obliged entity, VASP outside the AIFC is a subject to criminal, administrative liability and civil law measures in accordance with the legislation of Kazakhstan if they violate the AML/CFT legislation.

   However, liability measures for VASPs outside AIFC are limited to those that can be applied to other obliged entities given the specific nature of their activities, and the sanctions are not dissuasive and effective (see criterion 35.1).

   Subject to Par. 2.2 (c) of AIFC-FR0008, the AFSA is authorized to impose on obliged entities in AIFC, including VASP, disciplinary sanctions, law enforcement and other regulatory actions for violations related to AML/CFT. Sanctions involve a broad range of punishments (Par. 118 of AIFC Framework Regulations): a penalty (to an amount the AFSA thinks fit), conviction; payment of compensation; requesting for a report on unfounded enrichment or profit; termination or suspension of VASP business, instruction to rectify a violation; prohibition on holding offices or jobs at any AIFC organization.

   The amount of penal (financial) sanctions will depend on many factors and circumstances, as stated in Par. 6.4 to 6.33 of Chapter 6 of the AFSA Policy on Imposition of Financial Penalties, in particular, on violation gravity, presence of intent, type of subject that committed the violation, financial position of the person or organization that violated legal requirements, recurrence of violations, whether the offender faces financial difficulties, etc. When assigning punishment, the AFSA takes into account the actions taken in similar cases involving other persons. The AFSA does not use a "tariff system". Particular circumstances can justify the amount of financial penalty (Par. 6.18 of the said Policy). The AFSA has no criminal jurisdiction. In case of detection of criminal conduct, information shall be transferred to the relevant law enforcement authority and/or FIU of the Republic of Kazakhstan, also after internal infringement investigation procedures.

b) Subject to Par. 2.2 (c) of AIFC-FR0008 (as amended on December 12, 2021), the top management of VASP shall be responsible for observance of these rules. Moreover, the AFSA applies sanctions to persons which, proceeding from the "person" term definition, means any individual, legal or non-legal entity (the AIFC Glossary). Therefore, both legal entities and individuals being members of the AIFC shall be subject to sanctions (Paragraphs 118 to 121 of AIFC Framework Regulations).

   The procedure for applying sanctions to VASP outside AIFC is similar to that for other financial monitoring entities. No administrative sanctions shall be applied to officials (directors, senior management), unless the financial monitoring entity is a public or quasipublic organization (see Criterion 35.1(a)).

1518. **Criterion 15.9** Regardless of whether they operate within AIFC or outside AIFC, VASPs are

financial monitoring entities (Paragraphs 19 to 20 of Article 3 of the AML/CFT Law) and shall be subject to all AML/CFT requirements according to the AIFC laws or the laws of the Republic of Kazakhstan.

a) VASPs in AIFC have to apply CDD measures to each of their customers irrespectively of the amount of occasional transaction, and, in addition to this, VASPs are required to carry out a comprehensive CDD in respect of any customer who is classified as high risk (clauses (a) and (b) of para. 6.1.1. 6.1.1. AIFC-FR0008, para. 7.1.1. AIFC-FR0008), namely to verify the identity of the customer, its representative, any BO, obtain information on the purpose and nature of the business relationship, understand the sources of funds, wealth of the customer (par 6.2.2. AIFC-FR0008). Once the business relationship has been established, the VASP shall conduct CDD at any time if there is a suspicion of ML or doubts of the authenticity of the data previously provided by the customer when conducting CDD, or the risk of the customer has changed. The rules of Article 5(2) of the AML/CFT Law apply equally to VASPs outside AIFC.

   VASPs outside AIFC take CDD measures in the cases provided by Par. 2. Of Article 5 of the AML/CFT Law: i) establishing business relations with a client; ii) performing transactions in money and/or other assets, including suspicious transactions; iii) grounds for reasonable doubt about accuracy of previously received information on the client (representative thereof), beneficial owner;

b)

   i)-ii) AIFC laws provide for rules of electronic money transfers for AIFC members (Par. 11 of AIFC-FR0008).

   These rules apply to all obliged entities categories, including VASP. VASP in AIFC must retain the following information accompanying all electronic money transfers: compiler's name; sender's account number for transaction processing; sender's address or national identification number or the client's identification number, or date and place of birth; recipient's name; recipient's account number for transaction processing. In the absence of the account number, the unique reference number of the transaction should be specified for tracking the transaction (Paragraphs 11.2.1 to 11.2.2 of AIFC-FR0008).

   The ICR Requirements requires VASPs outside AIFC to have programmes on procedures for detecting cross-border payments and transfers of digital assets, as well as transfers within Kazakhstan (clause 20(4)). Given the specificity of the virtual asset sector and the existence of a notification procedure for the start of activities, the lack of requirements for transfers of digital assets in the Republic of Kazakhstan can be seen as a deficiency;

   iii)-iv) VASP shall be subject to requirements of Par. 12 of AIFC-FR0008 related to freezing and prohibiting transactions with persons and organizations put on the lists of persons linked to terrorist activities.

   VASP must create and maintain efficient control systems and means in order to ensure obtaining adequate information on a continuous basis about the relevant resolutions and sanctions adopted by the UNSC or by the Republic of Kazakhstan (Par. 12.1.1 of AIFC-FR0008).

   VASP must freeze money and other assets of designated individuals and legal entities according to the relevant resolutions and sanctions adopted by the UNSC or by the Republic of Kazakhstan immediately and without prior notice.

   VASP must observe the prohibition on transactions with the designated individuals and legal entities according to the obligations stated in the relevant resolutions and sanctions of the UNSC or lists of the Republic of Kazakhstan.

   Subject to Par. 12.1.1 of AIFC-FR0008, the requirements imposed on FI for freezing shall apply to "money", as well as to "other assets". The "other assets" can be broadly interpreted

taking into account subcl.2 cl.2 Art. 2 of the AML/CFT Law and AIFC legislation (see preamble to this section) and includes the "virtual assets" term.

The requirements of the AML/CFT Law in relation to the application of the TFS are fully applicable to VASPs outside AIFC (see Cr. 16.18), including the prohibition on informing.

1519. **Criterion 15.10** The procedure for FMA preparation (inclusion and removal), lists of entities and persons linked to TF and CPF, regulations on communicating to obliged entities, procedures for freezing and unfreezing transactions in money and/or other assets are provided in Article 12, Article 12-1, Par. 1-1 of Article 13 of the AML/CFT Law, as well as in Order 274 (see Criterion 6.5(d)). Regulations of these statutory acts cover VASP in and outside AIFC.

1520. When applying TFS, VASPs in and outside AIFC must meet the requirements of Par. 1-1 of Article 13 of the AML/CFT Law, namely: within 24 hours after placement of lists, immediately freeze transactions in money and/or other assets, including virtual assets, and provide information on or before the business day following the day of the relevant decision (action) of the financial monitoring entity by electronic means via dedicated links in Kazakh or Russian (Part 4 of Par. 2 of Article 13 of the AML/CFT Law).

1521. VASP in AIFC must notify the FMA of any frozen assets or actions taken in accordance with the prohibition requirements in the relevant resolutions and sanctions adopted by the UNSC or by the Republic of Kazakhstan, including attempts to perform transactions (Par. 12.1.2 of AIFC-FR0008).

1522. **Criterion 15.11** The Republic of Kazakhstan has a basis for international cooperation in AML/CFT (Chapter 3-1 of the AML/CFT Law, AIFC Cooperation and Exchange of Information Rules). Provisions of the AML/CFT Law and of the AIFC Cooperation and Exchange of Information Rules are applicable to cooperation under cases related to VASP and virtual assets.

1523. In particular, Article 19-1 of the AML/CFT Law provides for international cooperation in AML/CFT in terms of prevention, detection, suppression and investigation of acts, as well as forfeiture of criminal revenues between the FMA, other state authorities of the Republic of Kazakhstan and the relevant authorities of foreign states in accordance with the laws of the Republic of Kazakhstan, international treaties of the Republic of Kazakhstan and resolutions of the UNSC in accordance with the laws of the Republic of Kazakhstan. This cooperation builds on the principles of mutuality through requesting for and exchange of information.

1524. Subject to Article 19-4 of the AML/CFT Law, for AML/CFT purposes, as well as for purposes of searching, seizing, forfeiting and refunding money and/or assets obtained through crime, law enforcement and other special state authorities of the Republic of Kazakhstan shall engage in international cooperation at the time of field investigation activities, prejudicial inquiry, litigation and execution of court ruling, including exchange of information with the relevant authorities of foreign states.

1525. Based on the powers of the RK CPC, law enforcement authorities shall engage in international cooperation in AML/CFT with the relevant authorities of foreign states in the following forms: i) requesting for and obtaining of information, data and documents, as well as for purposes of searching, seizing, forfeiting and refunding money and/or assets obtained through crime; ii) providing assistance in searching, seizing, forfeiting and refunding money and/or assets, detection, suppression and investigation of ML/TF facts; iii) performing investigatory actions as part of prejudicial inquiry; iv) building investigation teams for joint international investigations.

1526. Article 19-3 of the AML/CFT Law provides for the following forms of cooperation of supervisory authorities in AML/CFT: i) obtaining and sending information on implementation of requirements of national laws; on obliged entities (activities, business reputation, management structure, beneficial owners); internal control programs, policy and procedures in AML/CFT; regulatory legal acts of the Republic of Kazakhstan; CDD results; ii) sharing experience and information related to regulation, control and supervision of obliged entities activities; iii) providing assistance and participating in monitoring over

obliged entities conducted by authorities of foreign states in the Republic of Kazakhstan.

1527. No regulations have been detected that would prevent international cooperation due to different status or subordination of supervisory authorities.

1528. Cooperation of the AFSA as a supervisory authority with regard to VASPs being members of the AIFC must ensure compliance of the AFSA with international standards of cooperation and information sharing developed for FI operating according to the basic principles, including the IOSCO Multilateral Memorandum of Understanding (MmoU), Enhanced MmoU of IOSCO and MmoU IAIS.

Weighting and Conclusion

1529. There are no requirements for exchange offices to identify or assess ML/TF risks for new products or to assess risks before launching new products, business practice or use of new or emerging technologies, that corresponds. General rules of the need for control and mitigation of identified risks are elaborated in the ICR of financial monitoring entities, including AIFC members.

1530. The AFSA assessed the ML/TF risks of virtual assets and VASPs sector as part of the NRA, however, vulnerability and risk analysis specific to AIFC members and not the VASPs generally in the country. The country takes certain measures for mitigation of the identified risks. However, risks of the use of VA and the activities of VASPs outside AIFC analysed weaker and measures to mitigate the risks identified were insufficient. Registration and license are required for operating as VASP within AIFC. VASP outside AIFC, that is a natural person, is not required to be registered or to obtain a license.

1531. If any risk is present, the AFSA shall establish all the BOs and their affiliates of VASPs, regardless of the ownership ratio. Measures preventing ownership and management are prescribed for VASP within AIFC. As for VASP outside AIFC, only management shall be subject to checking for no record of convictions. The BO and affiliates of the VASP outside AIFC are not checked for criminal records.

1532. The AFSA and MDD develop guidelines, however, the interaction is less about feedback for VASPs.

1533. VASP activities are subject to the required control and supervision. The AFSA and the MDD have a wide range of supervisory powers. The approach to supervision of VASP outside AIFC ignores the ML/TF risks. Managers or other officials of VASP outside AIFC are not subject to administrative sanctions, unless these organizations are quasipublic organizations.

1534. There are deficiencies in terms of compliance with requirements of R. 16 for VASP outside AIFC associated with lack of “travel rules “ for virtual assets as required by R.16. It is worth noting that there are no VASPs outside AIFC.

1535. **Recommendation 15 is rated partially compliant.**

Recommendation 16 – Wire transfers

1536. In the previous MER, the Republic of Kazakhstan was rated partially compliant with SR.VII in view of the fact that i) requirements that money transfers be accompanied by information about the sender were implemented only within the country rather than for international transfers; ii) there was no specific measure to monitor how banks comply with transfer operation rules; iii) the legislation is vague about transfer operations conducted by KazPost; iv) there is no requirement to have full information about the sender across the payment chain.

Sending Fis

1537. **Criterion 16.1**– When making cross-border (in favour of a foreign financial institution) wire payments and money transfers, the payment document should contain the following information (information should be accurate in light of CDD measures):

a) regarding the sender:

i) the first name, last name, patronymic (if any) or full or abbreviated names (for legal persons) of the money sender (para. 2 of Article 7 of the AML/CFT Law and subpara. I)-a of para. 11.2.3 of AIFC-FR0008);

ii) the individual identification code (para. 2 of Article 7 of the AML/CFT Law, para. 7 of Resolution No. 208 of the Management Board of the National Bank of Kazakhstan ("NB Resolution") or the account number of the sender (subpara. Ii)-a of para. 11.2.3 of AIFC-FR0008) if the money transfer is carried out through a bank account or the order number for the payment or money transfer (para. 2 of Article 7 of the AML/CFT Law) or the unique reference number of the transaction (subpara. Ii)-a of para. 11.2.3 of AIFC-FR0008) if the money transfer is carried out without a bank account;

iii) the identification code or address of the money sender or the number of the identity document of the money sender (para. 2 of Article 7 of the AML/CFT Law) or the identification number of the client or the date and place of birth (subpara. B of para. 11.2.3 of AIFC-FR0008).

b) regarding the recipient:

i) the first name, last name, patronymic (if any) or full or abbreviated names (for legal persons) of the money recipient (beneficiary) (para. 2 of Article 7 of the AML/CFT Law and subpara. Iii)-a of para. 11.2.3 of AIFC-FR0008);

ii) the individual identification code of the recipient (para. 2 of Article 7 of the AML/CFT Law) or the account number of the recipient (subpara. Iv)-a of para. 11.2.3 of AIFC-FR0008) if the money transfer is carried out through a bank account or the order number for the payment or money transfer (para. 2 of Article 7 of the AML/CFT Law) or the unique reference number of the transaction (subpara. Iv)-a of para. 11.2.3 of AIFC-FR0008) if the money transfer is carried out without a bank account.

1538. The requirements of the AML/CFT Law concerning information about the sender and recipient in the case of wire payments and money transfers in favour of a foreign financial institution (as amended on 1 July 2022) apply to banks, intermediary banks and postal service operators, when these make wire payments and money transfers in favour of a foreign financial institution, with the exception of payments and transfers through payment cards (para. 2 of Article 7 of the AML/CFT Law). See the AIFC Rules on ML/TF and Sanctions for wire transfer requirements applicable to FIs in AIFC.

1539. Other FIs authorised to make wire money transfers under Article 12 of Law 11-VI (payment organisations, organisations making settlements with transactions involving financial instruments) are subject to the requirements of Law 11-VI which refers to the AML/CFT Law (subpara. 2 of para. 12 of Article 13 of Law 11-VI). It is nevertheless not quite clear whether Law 11-VI applies to cross-border money transfers. At the same time payment organisations may make wire payments and money transfers in favour of a foreign financial institution only through STBs or KazPost. To be able to carry out its activities, payment organisations should have a partner bank without which the former cannot operate. Accordingly, the requirements of c.16.1 should be complied with by partner banks under para. 2 of Article 7 of the AML/CFT Law when it comes to cross-border transfers. The payment organisation does not transfer money on its own but rather sends necessary payment information to the partner bank.

1540. The legislation does not have an express requirement that the order for the payment or money transfer (if the money transfer is carried out without a bank account) allow for the tracking of the transaction. However, the NB Resolution of 17 September 2022 amended NB Resolution-208 concerning the procedure for conducting money transfers without opening a bank account which sets out that the sending bank assigns a unique number to the transaction and specifies this number in the document recorded in the international money transfer system when international payments are made.

1541. For FIs, the exception of payments and money transfers through payment cards is not limited to the

payment for goods and services which gives reason to conclude that the requirements to information about wire transfers do not extend to money transfers between natural persons through payment cards (para. 2 of Article 7 of the AML/CFT Law) which is inconsistent with R.16. The exception of payments and money transfers through payment cards is also not based on the requirement that the payment card number be specified in all transfers under the transaction. The Kazakh legislation on requirements to prepare a payment document when making transfers and payments through payment cards set out in NB Resolution-205 does not extend to international transactions. In this case the rules of international payment systems apply.

1542. Moreover, the requirements do not extend to a private client making debt payments under enforcement proceedings in favour of the state bodies using equipment designed to accept cash money.

1543. Also, the provisions of para. 2 of Article 7 of the AML/CFT Law do not extend to a private client conducting transactions under which money is credited to a bank account of a natural person or making payments in favour of a service provider using equipment designed to accept cash money and to a client making wire payments or money transfers without a bank account, but in such cases the transaction amount should not exceed KZT 500,000 (~EUR 1,000).

1544. **Criterion 16.2** – According to Law 11-VI (para. 3 of Article 31), when one sender makes wire payments or money transfers to several beneficiaries from one bank or when the sender's bank executes orders of several money senders in favour of one beneficiary, a summary payment order is allowed to be used. In this case the summary payment order made in hard copy is accompanied by a register of senders or beneficiaries as provided for by the regulation of the NB. According to NB Resolution-208 (paras. 21 and 22 and the Annex), the register has the number and date of the summary payment order to which the register is enclosed, as well as the details of the money senders or beneficiaries (name of the sender/beneficiary, individual identification code, individual identification number (business identification number), Code), the transfer amount broken down by money sender or beneficiary and the total transfer amount. Summary payment orders submitted in electronic form are made as per information transmission formats existing between the bank and its client, and no register is enclosed (para. 25 of NB Resolution-208).

1545. If several separate cross-border money transfers by one sender in favour of several beneficiaries are grouped into a single file, AIFC members should ensure that the single file contain information about the payer and information about the payment recipient for each payment recipient under c.16.1. This information should be fully traceable in the jurisdiction of each payment recipient (subpara. C of para. 11.2.3. of AIFC-FR0008).

1546. **Criterion 16.3** – Certain categories of cross-border transfers the amount of which does not exceed the minimum threshold of KZT 500,000, were excluded from the requirements of para. 2 of Article 7 of the AML/CFT Law. However, NB Resolution-208 applies to banks making cross-border payments (in favour of a foreign financial institution) which are excluded from para. 2 of Article 7 of the AML/CFT Law and requires the following information: transaction date, information about the sender and recipient, sending bank and recipient bank.

1547. Insofar as AIFC members are concerned, the requirements to provide information about the paying institution and recipient for wire payments the amount of which is below USD 1,000 include the sender's name, sender's account number used in the transaction (or the unique transaction number that allows for the tracking of the transaction if there is no account), recipient's name, recipient's account number used in the transaction (or the unique transaction number that allows for the tracking of the transaction if there is no account) (subpara. A of para. 11.2.3 of AIFC-FR0008).

1548. **Criterion 16.4** – The exclusion from the requirement regarding information accompanying cross-border wire transfers and the obligation to conduct CDD does not apply to suspicious transactions when the client makes a wire payment or transfers money without a bank account. According to subpara. 2) of para. 2 of Article 5 of the AML/CFT Law as amended on 1 July 2022 FIs conduct CDD when it comes to transactions involving funds and (or) other property, including suspicious transactions and verifying

obtained data. It is nevertheless unclear whether this also applies to transactions involving money credited to a bank account of a natural person or payments in favour of a service provider using equipment designed to accept cash money and debt payment transactions under enforcement proceedings in favour of the state bodies as this is not expressly enshrined in para. 3-1 of Article 5 of the AML/CFT Law.

1549. As for AIFC members, this requirement is set out in subpara. C of the last paragraph of para. 11.2.1 of AIFC-FR0008.

1550. **Criterion 16.5**– Payments and money transfers in the Republic of Kazakhstan should contain the details of the sender and recipient set out in the AML/CFT Law, with the exception of receipt of cash money for the purposes of making payments without opening a bank account and services involving the sale of electronic money and payment cards (para. 12 of Article 13 of Law 11-VI). The legislation is rather vague which identification information about the sender should accompany such transactions (whether NB Resolution-205 and NB Resolution-208 apply to such transactions) and whether this information is available to the receiving financial institution and relevant bodies through the use of other means.

1551. As for AIFC members, information about the paying institution and recipient of internal wire transfers should include information designated for cross-border wire transfers except for cases when this information may be available through the use of other means (subpara. D of para. 11.2.3 of AIFC-FR0008).

1552. Criterion 16.6 (partly met) – NB Resolution-208 (para. 7-1) provides for an opportunity for STBs, when making payments and money transfers through bank accounts, to include into the payment document an alternative identifier instead of recipient information. The alternative identifier means separate details, including alphanumerical characters making it possible to identify the client, make payments or money transfers through the payment system, and to track the transaction up to sender and recipient.

1553. However, there is no express obligation of the ordering FI to provide relevant identification information about the recipient to the competent bodies and FI of the recipient upon request. The ability of law enforcement authorities to compel FIs to provide such information immediately is not defined as well.

1554. As for AIFC members, the requirement under c.16.6 is established in subpara. 2, subpara. D of para. 11.2.3 of the Rules.

1555. **Criterion 16.7** – FIs are required to keep information that allows identifying the money sender and (or) recipient for five years since conducting the operation or closing customer's bank account.

1556. AIFC members should keep information about the sender and recipient in accordance with the general rules for keeping information in compliance with R.11 (subpara. E of para. 11.2.3 of AIFC-FR0008). See also the analysis of R.11.

1557. **Criterion 16.8** – The bank or OECTBO denies the order if the initiator fails to comply with the requirements to drafting and issuing orders or other requirements established by the Kazakh legislation (subpara. 3 of para. 7 of Article 46 of Law 11-VI). These requirements include the payment document having information about the payment or money transfer and the transfer of the details of the money sender and beneficiary as provided for by the AML/CFT Law (para. 12 of Article 13 of Law 11-VI).

1558. AIFC members should not make a wire transfer if they cannot comply with the requirements established by the legislation for wire transfers (subpara. F of para. 11.2.3 of AIFC-FR0008).

Intermediary financial institution

1559. **Criterion 16.9** – The requirements of para. 2 of Article 7 of the AML/CFT Law (as amended on 1 July 2022) regarding information about the sender and recipient of cross-border wire payments and money transfers apply to intermediary banks (STB and EECTBOs which make the payment and (or) money transfer received from the sender's bank in favour of a financial institution), including the requirements to keep information about the sender and recipient that accompanies the wire transfer (see the analysis of c.16.7).

1560. AIFC members that are intermediary institutions should keep all information about the sender and

recipient that accompanies the wire transfer (subpara. A of para. 11.2.4 of AIFC-FR0008).

1561. **Criterion 16.10** – Insofar as FIs are concerned, the legislation does not have any special provisions on keeping information obtained from the sending FI in cases when technical restrictions do not make it possible to keep the required information about the sender and recipient that accompanies the internal wire transfer. The provisions on keeping information under Law 11-VI and NB Resolution-208 (see the analysis of c.16.7) apply. No restrictions were found for banks and KazPost in terms of compliance with the requirements to keep information for five years after the account was closed. However, the provisions of these regulations do not extend to cross-border payments initiated abroad. As for AIFC members that are intermediary institutions, the requirements under c.16.10 are established in subpara. B of para. 11.2.4 of AIFC-FR0008.

1562. **Criterion 16.11** – The NB Resolution of 17 September 2022 amended NB Resolution-208 to the effect that the intermediary bank and recipient's bank, when making international payments and money transfers, ensure that automated data processing procedures be used to identify transactions that do not contain information about the sender and recipient as provided for by the Kazakh legislation or the rules of the international payment system. As for AIFC members that are intermediary institutions, the requirements under c.16.11 are established in subpara. C of para. 11.2.4 of AIFC-FR0008.

1563. **Criterion 16.12**– The NB Resolution of 17 September 2022 amended NB Resolution-208 to the effect that the intermediary bank should have in place internal procedures that determine the bank's rules of procedure (execution, denial, suspension) based on the ML/TF risk assessment when it receives a payment order without the details of the sender or recipient. As for AIFC members that are intermediary institutions, the requirements under c.16.12 are established in para. 11.2.6 of AIFC-FR0008.

Receiving financial institution

1564. **Criterion 16.13**– STBs and OECTBOs, as well as intermediary banks and postal service operators, control that the payment document should have the required information about the sender and recipient when the payment and money transfer is received from a foreign financial institution (para. 2 of Article 7 of the AML/CFT Law), which makes it possible to conclude that these Fis should take necessary action to identify wire transfers that do not have the required information about the recipient or the required information about the sender.

1565. However, the legislation has certain flaws identified in the analysis of c.16.1 and related to transactions which were excluded from the requirements about information that should accompany cross-border wire transfers.

1566. When sending or receiving money through a wire transfer on behalf of the client, AIFC members should ensure that the wire transfer and any correspondence associated with it contain accurate information about the sender and recipient and control wire transfers in order to identify those wire transfers that do not have information about the sender and recipient and take necessary action to identify any ML risks (subpara. A of para. 11.2.5 of AIFC-FR0008).

1567. **Criterion 16.14** – The AML/CFT Law does not have any special provisions for receiving institutions to verify the recipient's personal details when making a cross-border wire transfer with the amount of USD 1.000 and more, but common requirements shall be applied on taking CDD measures before making money transactions, including verifying the accuracy of information required to identify the client, with the exception of cases when such measures were taken when establishing business relations (para. 1 of Article 7 of the AML/CFT Law).

1568. When sending or receiving money through a wire transfer on behalf of the client, AIFC members should ensure that the wire transfer and any correspondence associated with it contain accurate information about the recipient (subpara. B of para. 11.2.5 of AIFC-FR0008).

1569. There are no specific provisions for wire transfers regarding the retention of information, but general provisions apply to keeping the documents and data obtained following CDD for at least five years since

the business relations with the client were terminated (para. 4 of Article 11 of the AML/CFT Law).

1570. C**riterion 16.15** – The NB Resolution of 17 September 2022 amended NB Resolution-208 to the effect that banks (including KazPost) should have in place internal procedures to decide in reliance on the ML/TF/PF risk assessment (i) when to execute, deny or suspend a wire transfer that does not have the required information about the sender or the required information about the recipient; and (ii) what further action to take. There also apply general provisions to the effect that the order is denied if the requirements to drafting and issuing orders or other requirements are not complied with (subpara. 3 of para. 7 of Article 46 of Law 11-VI), but these provisions are not based on the RBA. There also apply general risk management and internal controls procedures for STBs under the risk management system rules for banks that establish a procedure for denying high ML/TF risk transactions and terminating business relations with the client based on inherent risk factors.

1571. As for AIFC members, the requirements under c.16.15 are established in para. 11.2.6 of AIFC-FR0008.

MVTS operators

1572. **Criterion 16.16** – As for Fis, the AML/CFT Law does not establish any specific MVTS requirements in terms of wire payments and money transfers and, accordingly, any obligation to comply with the requirements of R.16 in countries they operate directly or through their agents. There apply general requirements to Fis which are authorised, among other things, to provide MVTS (STBs, OECTBOs (KazPost), payment organisations).

1573. As it follows from the analysis of c.16.1, the requirements of the AML/CFT Law relating to information about the sender and recipient of wire transfers apply to banks and OECTBOs, as well as postal service operators. Law 11-VI applies to other Fis, but this law extends only to actions relating to international payments and money transfers initiated and executed in the Republic of Kazakhstan (para. 2 of Article 2 of Law 11-VI). At the same time practice shows that these Fis are not authorised to provide MVTS in foreign jurisdictions directly or through their agents but are obliged to have the legal person registered and licensed in accordance with the requirements of other countries. According to the AML/CFT Law (para. 3-1 of Article 11), obliged entities ensure that all their branches and subsidiaries comply with the ICR.

1574. The requirements of Law 11-VI relating to information that accompanies wire transfers also extend to the paying agent or paying subagent of the bank, OECTBO, and payment organisation (this agent or subagent is a payment service provider and as such covered by Law 11-VI).

1575. As for AIFC members, the requirements under c.16.16 are established in subpara. A of para. 11.2.7 of AIFC-FR0008.

1576. **Criterion 16.17** – The legislation does not provide for an express obligation for MTVS providers that control the sending and receiving ends of the wire transfer to submit an STR in any country to which the suspicious wire transfer relates. Accordingly, the requirements of the AML/CFT Law for Fis (including MVTS) to immediately report a suspicious transaction to the Kazakh authorised body do not extend to the authorised bodies of other countries but rather to the Kazakh authorised body. The FMA, in turn, may inform the authorised bodies of other countries as part of international cooperation.

1577. As for AIFC members, the requirements under c.16.17 are established in subpara. B of para. 11.2.7 of AIFC-FR0008.

Application of targeted financial sanctions

1578. **Criterion 16.18** – Insofar as persons and organisations involved in terrorism, terrorist and extremist financing, as well as those involved in proliferation financing, FIs are obliged, within twenty-four hours, to take action to freeze transactions involving funds or other property, including denial of transactions involving funds or other property, committed by such an organisation or natural person, or in their favour,

as well as by the client whose beneficiary owner is such a natural person (para. 1.1 of Article 13 of the AML/CFT Law). Transaction freezing measures do not apply to the extension of bank deposits and crediting and transfer of money from the person's bank account, in discharge of his obligations under bank loan, leasing, or microcredit agreements entered into before the person was designated as a person involved in terrorist and extremist financing.

1579. The transaction freezing requirements for FIs concern persons listed on the authorised body's website. Grounds for designating an organisation or natural person as an organisation and person involved in terrorist and extremist financing include, but not limited to, the application of UNSC target financial sanctions against the person or the inclusion of the organisation or natural person into sanctions lists made by UNSC committees and relating to the prevention and suppression of terrorism and terrorist financing (subpara. 7 of para. 4 of Article 12 of the AML/CFT Law).

1580. AIFC members should establish and maintain effective control systems and means in order to ensure that it will be properly informed about the relevant resolutions or sanctions adopted by the UNSC or Republic of Kazakhstan and it will take reasonable steps to comply with the same. The relevant person should immediately and without prior notice freeze the funds or other assets of the specified natural and legal persons and comply with prohibitions to conduct transactions with the identified persons and organisations in compliance with the obligations set forth in the relevant resolutions or sanctions adopted by the UNSC or Republic of Kazakhstan (para. 12.1.1 of AIFC-FR0008).

Weighting and Conclusion

1581. Most requirements of R.16 are complied with. However, there are certain deficiencies, including those relating to transactions excluded from the requirements concerning information that should accompany cross-border wire transfers, information about wire payments below the threshold, as well as the requirements to keep all necessary information.

1582. **R.16 is rated largely compliant.**

Recommendation 17 – Reliance on third parties

1583. In the previous MER, the former R.9 was not recognized.

1584. **Criterion 17.1** – FIs (with the exception of the postal service operator and persons engaged in licensing activities as a licensor without a license) may rely that other FIs and DNFBPs, as well as foreign financial institutions, apply (a)–(c) items of CDD measures established in R.10 in respect of the relevant clients and BOs (para. 6 of Article 5 of the AML/CFT Law).

1585. However, there is no provision in the legislation that in this case FIs take ultimate responsibility for compliance with the requirements to CDD of clients and BOs on the part of third parties.

1586. AIFC members may rely on certain third parties listed in para. 9.1.1 of AIFC-FR0008 in terms of implementing one or several items of CDD on their behalf and also rely on information previously obtained by the third party that coves one or several items of CDD (paras. 9.1.2 and 9.1.2 of AIFC-FR0008). Reliance on third parties to take CDD measures is not therefore limited to (a)–(c) items of R.10 but also extends to d) element, and AIFC members can rely on third parties to perform ongoing monitor the business relationship which is non-compliant with R.17.

1587. The AIFC member remains responsible for compliance and is held liable for any non-compliance with the CDD requirements (para. 9.1.6 of AIFC-FR0008).

a) FIs should immediately receive information about the client, BO, including copies of supporting documents to the extent of measures under a)–(c) items of R.10 (subpara. 1) of para. 6 of Article 8 of the AML/CFT Law, cl. a) par. 9.1.3 AIFC-FR0008).

b) FIs, as well as AIFC members, shall immediately take necessary steps to have a possibility to obtain copies of supporting documents in accordance with the CDD requirements (subpara. 1) of para. 6 of Article 8 of the AML/CFT Law, cl. «b» para. 9.1.3 AIFC-FR0008).

c) In relation to FIs outside AIFC the requirements of c.17.1 c) extend only to third parties that are foreign FIs (para. 6 of Article 5 of the AML/CFT Law). As for third parties of FIs and DNFBPs outside AIFC, the CDD and data keeping requirements are set forth in Articles 5 and 11 of the AML/CFT Law since these entities are obliged entities, and they are supervised and monitored.

The FI in AIFC should ensure that the third party:

- apply the necessary CDD measures, including those related to client identification and record keeping (subpara. A-a of para. 9.1.3 of AIFC-FR0008);
- is subject to regulation by the financial service body or other competent body in a country in which there exist rules equivalent to standards set forth in the FATF Recommendations, and that the third party is monitored for compliance with such rules, and whether the third party did not rely on a certain exclusion from the requirement to implement certain relevant items of CDD (subpara. C of para. 9.1.3 of AIFC-FR0008).

1588. **Criterion 17.2** – FIs may not rely on third parties taking CDD measures in cases when the third party is registered, present or stays in a country that does not or insufficiently complies with the FATF Recommendations (subpara. 3 of para. 10 of Article 5 of the AML/CFT Law as amended on 1 July 2022).

1589. Further, the FI that instructed a foreign financial institution to take CDD measures under an agreement should factor into potential AML/CFT risks (para. 8 of Article 5 of the AML/CFT Law as amended on 1 July 2022).

1590. If the AIFC relies on a third party situated in a foreign jurisdiction, including the Republic of Kazakhstan, to implement one or several items of CDD, the FI should ensure that the AML/CFT requirements consistent with the FATF Standards apply there (subparas. F) and g) of para. 9.1.6. of AIFC-FR0008).

1591. **Criterion 17.3** – The FI which is a member of a financial group may also rely on CDD measures taken by other members of that group provided that the requirements of the AML/CFT Law are complied with under c.17.1 and that the members of the group comply with the ICR of the relevant FI and that the responsible organisation of the group (the competent body at the group-wide level) implement and ensure compliance with the ICR of the relevant FI on the part of the members of the group (para. 6-1 of Article 5 of the AML/CFT Law as amended on 1 July 2022). These conditions are not entirely consistent with c.17.3 since it is not provided that any higher country risk is fully offset by the AML/CFT mechanisms of that group.

1592. If the AIFC member relies on a member of its Group, this member of the Group should not be subject to regulation by the supervisory or other competent body in a country in which there exist AML/CFT rules equivalent to standards set forth in the FATF Recommendations and should not be monitored for compliance with these rules if:

a) the Group pursues and implements a group-wide CDD and recording policy that is equivalent to standards set forth in the FATF Recommendations (para. 9.1.4 of AIFC-FR0008) and;

b) if effective compliance with the requirements to CDD and recording and AML/CFT programmes is monitored at the Group-wide level by the supervisory or other competent body in a country in which there exist rules equivalent to standards set forth in the FATF Recommendations;

c) the Group's AML policy appropriately mitigates any factors of higher geographic risks.

Weighting and Conclusion

1593. The legislation allows FIs to rely on other obliged entities and foreign FIs to implement (a)–(c) items

of CDD measures in R.10 but all the conditions set forth in R.17 are not met. Furthermore, AIFC members may rely on third parties to perform constant monitoring of business relations which is non-compliant with R.17.

1594. **R.17 is rated largely compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

1595. In the previous MER, the Republic of Kazakhstan was rated partially compliant and non-compliant with the former R.15 and R.22 respectively. The reason for that lay in the absence of requirements:

i) in respect of consumer credit cooperatives; pawnshops; microcredit organisations; licensing companies; insurance agents; organisations that accept cash from customers as payment for services provided by the attorney acting on behalf and at the direction of the principal (service provider) under an agency agreement, including through electronic terminals;

ii) to the appointment of a special official responsible for the implementation of the AML/CFT policy and rules in FIs (with the exception of banks);

iii) to FIs in terms of the qualification, instruction and training of personnel involved in AML/CFT;

iv) to screening procedures applied to all FIs' personnel upon hiring;

v) to bringing the ICR to the attention of FIs' personnel;

vi) of the AML/CFT legislation in relation to subsidiaries and branches.

1596. **Criterion 18.1**– FIs elaborate, adopt and implement the ICR and programmes of their implementation which should include an internal controls organisation programme for the purposes of AML/CFT and an ML/TF risk management programme that takes into account the degree of vulnerability of FIs' services to ML/TF risks, as well as the size, nature and complexity of organisation (subparas. 2 and 3 of Article 11 of the AML/CFT Law).

1597. Specific requirements to AML/CFT programmes for FIs may be found in the relevant ICR requirements for each category of FIs. The ICR requirements vary across FIs insofar as internal controls are concerned.

a) According to para. 3 of Article 11 of the AML/CFT Law (as amended on 1 July 2022) and the relevant ICR Requirements (para. 5 of the ICR for STBs, para. 5 of the ICR for unified accumulative pension funds (UAPF), para. 9 of the ICR for the non-financial sector, para. 5 of the ICR for exchange offices, para. 5 of the ICR for payment organisations, para. 5 of the ICR for the securities market, para. 5 of the ICR for stock exchanges, para. 5 of the ICR for microfinancing organisations, para. 9 of the ICR for the post, para. 9 of the ICR for commodity exchanges, para. 5 of the ICR for insurers, para. 5 of the ICR for the AIFC), FIs appoint a senior manager responsible for the implementation of and compliance with controls and choose the FI's division or employees to which competence AML/CFT matters fall. The AML/CFT internal controls organisation programme includes a description of the functions of the AML/CFT division, as well as the functions and powers of the responsible employee of the AML/CFT division.

b) According to para. 3 of Article 11 of the AML/CFT Law (as amended on 1 July 2022), the internal controls organisation programme should contain requirements to FIs' employees responsible for the implementation of and compliance with the ICR, including a requirement to have unblemished business reputation. However, with the exception of AIFC members, the ICR Requirements contain only provisions that relate to maintaining standards when hiring the responsible employee who monitors compliance with the ICR and do not require the AML/CFT programmes for FIs to have mandatory screening procedures to ensure high standards when hiring all employees of FIs.

Further, the ICR Requirements for FIs vary in standards applicable to the responsible employee. All FIs are required to have unblemished business reputation but it is not always necessary to have working experience as head or working experience in the AML/CFT area.

For instance, the responsible employee of STBs should have a higher education and at least one year of working experience as head of a division of a bank that deals with banking or other transactions or at least two years of working experience in the AML/CFT area or at least three years of working experience in the regulation of financial services (para. 5 of the ICR for STBs).

Only AIFC members are required to implement screening procedures to ensure high standards when hiring employees (para. 14.1.1 of AIFC-FR0008).

c) The ICR for FIs should include an AML/CFT instruction and training programme (para. 3 of Article 11 of the AML/CFT Law, para. 14.1 of AIFC-FR0008).

The relevant ICR Requirements for all FIs contain provisions regarding the AML/CFT instruction and training programme, including objectives, content and frequency (para. 33 of the ICR for the AIFC, para. 36 of the ICR for the non-financial sector, para. 39 of the ICR for commodity exchanges, para. 33 of the ICR for stock exchanges, para. 33 of the ICR for payment organisations, para. 31 of the ICR for microfinancing organisations, para. 24 of the ICR for UAPFs, para. 34 of the ICR for STBs, para. 36 of the ICR for insurers, para. 38 of the ICR for exchange offices, para. 35 of the ICR for the securities market).

The ICR Requirements for all FIs also refer to the requirements to instruct and train personnel approved by the authorised financial monitoring body in accordance with para. 8 of Article 11 of the AML/CFT Law.

d) According to the ICR Requirements for all FIs, AML/CFT internal controls organisation involves the elaboration of the ICR which include requirements for the internal audit service to assess the effectiveness of AML/CFT internal controls (para. 4 of the ICR for STBs, para. 4 of the ICR for UAPFs, para. 3 of the ICR for the non-financial sector, para. 4 of the ICR for exchange offices, para. 4 of the ICR for microfinancing organisations, para. 4 of the ICR for payment organisations, para. 6 of the ICR for the post, para. 4 of the ICR for the securities market, para. 4 of the ICR for the AIFC, para. 4 of the ICR for insurers, para. 6 of the ICR for commodity exchanges, para. 4 of the ICR for stock exchanges).

Additionally, AIFC members should ensure that the audit include regular inspections and effectiveness assessments of AML policy, procedures, control systems and means (para. 14.6.1 of AIFC-FR0008).

The functions of the responsible employee and those of employees of the AML/CFT division are not combined with the functions of the internal audit service (para. 11 of the ICR for STBs, para. 13 of the ICR for the non-financial sector, para. 11 of the ICR for payment organisations, para. 16 of the ICR for the post, para. 10 of the ICR for insurers, para. 9 of the ICR for stock exchanges, para. 10 of the ICR for the securities market, para. 10 of the ICR for microfinancing organisations, para. 10 of the ICR for UAPFs, para. 11 of the ICR for the AIFC, para. 11 of the ICR for exchange offices, para. 16 of the ICR for commodity exchanges).

1598. **Criterion 18.2** – FIs ensure that its branches, representative offices, subsidiaries situated either in the Republic of Kazakhstan or abroad comply and implement the ICR unless it contradicts the legislation of the country they are situated in (para. 3-1 of Article 11 of the AML/CFT Law). Besides, FIs that are members of a financial group may elaborate, adopt and implement the ICR for this financial group, taking into account the specifics and features of its members (para. 3 of Article 11 of the AML/CFT Law as amended on 1 July 2022).

1599. According to the relevant ICR Requirements for certain FIs, AML/CFT internal controls organisation programmes should contain a procedure for complying with and implementing the ICR on the part of its

branches, representative offices, subsidiaries situated either in the Republic of Kazakhstan or abroad unless it contradicts the legislation of the country they are situated in (subpara. 8 of para. 7 of the ICR for STBs, subpara. 9 of para. 8 of the ICR for UAPFs, subpara. 8 of para. 8 of the ICR for the non-financial sector, subpara. 9 of para. 6 of the ICR for microfinancing organisations, subpara. 9 of para. 6 of the ICR for the securities market, subpara. 9 of para. 6 of the ICR for insurers).

1600. AIFS members should ensure that their policy, procedures, control systems and means be applied to all branches or subsidiaries of the AIFC member outside the AIFC jurisdiction and to all enterprises of the Group of Companies that are AIFC members (para. 14.2.1 of AIFC-FR0008).

1601. There is nevertheless no obligation to have compliance, audit, and AML/CFT functions at the group-wide level, as well as to ensure that customer, account and transaction information is exchanged between branches and subsidiaries, and to share the compliance, audit and AML/CFT functions at group level.

a) The relevant ICR requirements for FIs (with the exception of stock exchanges and AIFC) set out that AML/CFT internal controls organisation programmes should contain a procedure for cooperation with other divisions of the FI, branches, subsidiaries in the course of AML/CFT control (subpara. 7 of para. 7 of the ICR for STBs, para. 8 of the ICR for UAPFs, subpara. 7 of para. 8 of the ICR for the non-financial sector, subpara. 1 of para. 7 of the ICR for exchange offices, subpara. 8. Of para. 6 of the ICR for microfinance organisations, subpara. 1 of para. 7 of the ICR for payment organisations, subpara. 6 of para. 11 of the ICR for the post, subpara. 8 of para. 6 of the ICR for the securities market, subpara. 8 of para. 6 of the ICR for insurers, subpara. 7 of para. 11 of the ICR for commodity exchanges).

   AIFC members that are part of the Group should understand policy and procedures relating to information exchange between the enterprises of the Group of Companies, especially when exchanging information about CDD and should have proper assurances of confidentiality and use of information exchanged by the enterprises of the Group of Companies, including compliance with the relevant data protection legislation (para. 14.3.1 of AIFC-FR0008).

   Fis, however, are not specifically required to include into group-wide programmes the principles of policy and procedures of exchanging information necessary for the purposes of CDD and ML/TF risk management.

b) Aside from the right of FIs that are members of a financial group to exchange information and documents obtained during internal controls (para. 6 of Article 11 of the AML/CFT Law as amended on 1 July 2022), legal acts have no express obligation for FIs, with the exception of AIFC members, to ensure that information about the client, account and transactions be exchanged among branches and subsidiaries and compliance, audit, and AML/CFT functions at the group-wide level.

   AIFC members that are part of the Group should provide information about the clients' accounts and transactions from branches and subsidiaries (para. 14.3.1 of AIFC-FR0008).

c) Legal acts have no express obligation for FIs, with the exception of AIFC members, to include into the AML/CFT group-wide programme measures of proper protection of confidentiality and use of information including protection to prevent leakages of information exchanged by the members of the group.

   AIFC members that are part of the Group should have proper assurances of confidentiality and use of information exchanged by the enterprises of the Group of Companies, including compliance with the relevant data protection legislation (para. 14.3.1 of AIFC-FR0008).

1602. Criterion 18.3 (met) – FIs ensure that its branches, representative offices, subsidiaries situated either in the Republic of Kazakhstan or abroad comply and implement the ICR unless it contradicts the legislation of the country they are situated in, and are also obliged to report to the authorised body and control and supervisory bodies any inabilities to comply with and implement the ICR beyond the Republic of Kazakhstan and to take additional action to manage and mitigate AML/CFT risks (para. 3-1 of Article 11

of the AML/CFT Law).

1603. This obligation extends to AIFC members if the relevant branch, subsidiary or enterprises of the Group are not subject to regulation equivalent to the FATF Standards and are not monitored for compliance with such rules (paras. 14.2.1 and 14.2.2 of AIFC-FR0008).

Weighting and Conclusion

1604. FIs are obliged to implement ML/TF risk management programmes but these do not have all necessary items of R.18, including information exchange and compliance, audit, and AML/CFT functions at the group-wide level

1605. **R.18 is rated largely compliant.**

Recommendation 19 – Higher risk countries

1606. In the previous MER, the Republic of Kazakhstan was rated non-compliant with the former R.21 in view of the fact that i) the term "non-cooperative states" was not regulated and there was no obligation to pay special attention to transactions involving persons from such countries; ii) there was no requirement to examine transactions involving persons from "non-cooperative states" and to keep information for submission to the authorised body or auditor; iii) there were no countermeasures against countries that do not or insufficiently comply with the FATF Recommendations.

1607. **Criterion 19.1** – As part of CDD, FIs are obliged to take additional EDD measures in respect of persons who are registered, reside or stay in a state (territory) that does not or insufficiently complies with the FATF Recommendations (see the analysis of c.10.17), as well as to revise or, if need be, to terminate correspondent relations with FIs (para. 10 of Article 5 of the AML/CFT Law).

1608. In particular, FIs may not rely on CDD measures taken by other obliged entities and foreign financial institutions and instruct other persons to take CDD measures upon establishing business relations with a person who is registered, resides or stays in a state (territory) that does not or insufficiently complies with the FATF Recommendations (para. 10 of Article 5 of the AML/CFT Law).

1609. Moreover, FIs are obliged to review the transactions of their clients in cases when a transaction is conducted by a person who is registered or resides in a state (territory) that does not or insufficiently complies with the FATF Recommendations and when an account in a bank registered in such a state is involved (para. 4 of Article 4 of the AML/CFT Law).

1610. According to the relevant ICR Requirements for FIs, foreign states, transactions with which increase ML/TF risks and in respect of which EDD measures are taken, include, but not limited to, foreign states included in a list of states that do not or insufficiently comply with the FATF Recommendations

1611. **Criterion 19.2** – The Inter-Agency AML/CFT Council reviews FATF calls and makes decisions to mitigate ML/TF risks (para. 4 of Article 11-1 of the AML/CFT Law). The authorised body reports risk mitigation decisions to FIs.

1612. The Inter-Agency Council may also recommend that the state bodies reduce internal ML/TF risks and may assess the implementation of such recommendations (para. 4 of Article 11-1 of the AML/CFT Law) irrespective of FATF calls. At the same time measures taken irrespective of FATF calls are not binding in nature but are recommendations.

1613. Criterion 19.3 (met) – The FIU brings decisions to mitigate ML/TF risks identified by FATF to the attention of FIs (para. 4 of Article 11-1 of the AML/CFT Law). The authorised body makes a list of states that do not or insufficiently comply with the FATF Recommendations relying on the documents published by FATF on its website (para. 4 of Article 4 of the AML/CFT Law).

Weighting and Conclusion

1614. The legislation generally complies with R.19. FIs are obliged to take EDD measures in relation to

business relations and transactions involving natural and legal persons from countries against which FATF makes its calls. The Kazakh bodies may take relevant countermeasures if these are called for by FATF and irrespective of such FATF calls and inform FIs to this effect. There are insignificant deficiencies with the absence of requirements to the proportionality of measures taken against risks.

1615. **R.19 is rated largely compliant.**

Recommendation 20 – Reporting of suspicious transactions

1616. In the previous MER, the Republic of Kazakhstan was rated non-compliant with the former R.13 which was due to the fact that: i) there was no express obligation to file STRs on suspicion of ML; ii) the AML/CFT requirements did not extend to credit consumer cooperatives; pawnshops; microcredit organisations; leasing companies; insurance agents; organisations that accept cash from customers as payment for services provided by the attorney acting on behalf and at the direction of the principal (service provider) under an agency agreement, including through electronic terminals; and iii) there was no requirement to file STRs when attempts to conduct ML-related transactions are made.

General information

1617. Instructions to report transactions involving funds and (or) other property when these are declared suspicious are set forth in the AML/CFT Law, the requirements of which extend to all categories of obliged entities, including AIFC obliged entities. The regulatory provisions are specified in detail in the ICR requirements for all categories of obliged entities, the AIFC Rules on ML/TF and Sanctions.

1618. **Criterion 20.1** – The AML/CFT Law obligates obliged entities to immediately report suspicious transactions to the FMA before conducting them (para. 2 of Article 13) and to provide the FMA with information and data about transactions subject to financial monitoring (Article 10). When a transaction is declared suspicious after it was conducted, a report that the transaction was conducted is filed to the FMA no later than twenty-four hours after the transaction was declared suspicious.

1619. To declare a transaction suspicious, it is necessary to have suspicions that funds and (or) other property involved in the transaction are criminal proceeds or that ML/TF or other criminal activities are the purposes of the transaction itself (subpara. 1) of Article 1 of the AML/CFT Law).

1620. **Criterion 20.2** – A suspicious transaction involving funds and (or) other property is a transaction of a client (including an attempt to conduct such a transaction, a transaction in the process of being conducted or a transaction that has already been conducted) in relation to which there arise suspicions that funds and (or) other property involved in the transaction are criminal proceeds or that ML/TF or other criminal activities are the purposes of the transaction itself (para. 1) of part. 1 of Article 1 of the AML/CFT Law).

1621. Suspicious transactions are subject to financial monitoring irrespective of how they are conducted and the amount that was involved or could have been involved in such transactions (para. 3 of Article 4 and para. 2 of Article 13).

Weighting and Conclusion

1622. **R.20 is rated compliant.**

Recommendation 21 – Tipping-off and confidentiality

1623. In the previous MER, the Republic of Kazakhstan was rated as Largely Compliant according to the outdated Recommendation 14. The identified shortcomings were due to the fact that no requirement had been placed on FI directors, officers and employees to inform their clients and other persons that any information concerning them was submitted to an authorized unit.

1624. **Criterion 21.1** – Submission to an authorized financial monitoring unit of any FI-related information and documents for the purposes and in the manner set out in the AML/CFT Law is not deemed to be

disclosure of proprietary, commercial, banking or any other secrecy protected by law (clause 6, article 11 of the AML/CFT Law, and clause 13.7.4 of AIFC-FR0008). Where any information or documents have been submitted to an authorized unit as required by the AML/CFT Law, regardless of any consequences of such submission, the respective FI, its officers and employees are not held liable in the manner consistent with the relevant laws of the Republic of Kazakhstan and the respective civil contract (clause 7, article 11 of the AML/CRFT, and clause 14.8.1. of AIFC-FR0008). Nor any reference is made to other regulations, specifically administrative instruments, but it follows from the information provided by the Republic of Kazakhstan that criminal liability for information disclosure may be enforced only to the extent permitted by law.

1625. **Criterion 21.2** – It is not allowed to inform clients or other persons on any measures of anti-money laundering, counter financing of terrorism and counter financing of proliferation applied towards such clients or other persons other than letting clients know respective action taken to put on hold any transactions involving money and (or) any other property, interdicting the establishing of business relations or the undertaking of any transactions involving money and (or) any other property (clause 5, article 11 of the AML/CFT Law, 'Guidance on Tipping-off' in the final part of section 13.7 of AIFC-FR0008).

Weighting and Conclusion

1626. Submission of information to an authorized unit in accordance with the AML/CFT Law does not qualify for a legal non-compliance under Kazakh law while FI officers and employees are protected from criminal and civil liability. It is disallowed to apprise clients and other persons of any client information, data or documents submitted to an authorized unit or any transactions undertaken by them.

1627. **Recommendation 21 is rated compliant.**

Recommendation 22 – DNFBPs: customer due diligence

1628. In the previous MER, the Republic of Kazakhstan was rated as 'Non-compliant' according to the outdated Recommendation 12 due to material shortcomings identified in the outdated Recommendations 5, 6, and 8-11.

1629. C**riterion 22.1** – The CDD requirements covering all DNFBP categories apply when: i) business relations are established; ii) transactions involving money and (or) other property, including suspicious transactions are undertaken; iii) there are some doubts over relevant information obtained on the client (its representative), the BO (clause 2, article 5 of the AML/CFT Law). The minor deficiencies identified in R.10 also apply to DNFBPs in terms of not being able to conduct CDD but to send STR to the FMA. The CDD requirements apply to DNFBPs:

a) casinos must carry out CDD casinos must conduct CDD of the customers (their representatives) and BOs before establishing the business (Art. 6 of the AML/CFT Law); and AML/CFT Law); as well as in cases of: transactions, including suspicious transactions (when the amount of winnings equals or exceeds 1.000.000 KZT (~USD 2,1 thousand)); existence of reasons to doubt the reliability of previously obtained information about the customer (its representative) and BO, when conducting (attempting to conduct) suspicious transaction, making unusual transactions (sub-par. 2, 3, 4 of par. 1 of cl. 31 of the ICR Requirements for Organisers of Gambling Industry and Lotteries). However there are no requirements assuring that a casino may link any information obtained at individual client due diligence to a transaction that such client undertakes at a casino.

   The e-casino and online-casino business are prohibited in the Republic of Kazakhstan (sub-clauses 2) clause 2, article 6 Law of the Republic of Kazakhstan-219-PP). There are no ship-based casinos in Kazakhstan;

b) real estate agents carry out due diligence of clients (their representatives) and BOs as required by clause 2 and clause 4, article 5 of the AML/CFT Law, sub-clauses 10, clause 8 of the ICR

requirements for the financial sector and when transactions valued at or above KZT 50,000,000 (USD 102,800) are undertaken (sub-clause 8) part 1, article 4 of the AML/CFT Law);

The obligations binding on AIFC members, being either developers or agencies that undertake real estate sale and purchase transactions with clients (sub-clause 1, clause 5 of the List of Financial and Ancillary Services offered by AIFC members subject to financial monitoring, CDD measures are to be implemented towards identifying the client and any person acting on behalf of a client and any beneficial owner (sub-clause (a), (a-a) clause 6.3.1, section 6 of AIFC-FR0008) where the client undertakes occasional transactions or related transactions (at that or later time) individually or collectively valued at or above USD 15,000; and towards: (i) each client classified as a high-risk client; (ii) business relations and transactions with persons originating from countries carrying high geographical risks (sub-clauses 6.1.1., section 6 of AIFC-FR0008).

The aforementioned obliged entities categories are not bound to implement CDD measures for both buyers and sellers.

c) dealers in precious metals and stones and associated jewelry items, pawnshops implement CDD measures as required by clause 2, article 5 of the AML/CFT Law and when a one-off transaction is undertaken valued at or above KZT 500,000 (~USD 1,3000), when precious metals & gems associated jewelry items are sold and purchased valued at KZT 5,000,000 (equivalent to about USD 10,300) with pawn shops carrying out CDD for transactions valued at KZT 3,000,000 (equivalent to ~ USD 6,200).

   AIFC members, i.e. precious metal or stones dealers (no threshold transaction value is set) (sub-clause 2, clause 5 of the Financial Service and Ancillary Services offered by AIFC members subject to financial monitoring) and dealers of any item on sale (including precious metals or gems) priced at or above USD 15,000 (sub-clause 3, clause 5 of the Financial Service and Ancillary Services offered by AIFC members subject to financial monitoring) implement CDD measures where AIFC members, being developers and agencies, that undertake real estate sale and purchase transactions with clients, are required to do so;

d) lawyers, legal advisors and other independent legal professionals conduct CDD measures where they act in on transactions involving money and (or) other property for or on behalf of the client as part of the following activities: i) real estate sale and purchase; ii) management of client's money, securities or other property; iii) management of bank accounts or securities accounts; iv) accumulation of funds for creating, maintaining, keeping operational, and managing a company; v) incorporation, selling & acquisition, sustenance and management of a legal entity (sub-clause 7), clause 1, article 3 of the AML/CFT Law). Also the notaries carrying out notarial acts involving money and/or other property (Article 3(1)(6) of the AML/CFT Law) as well as accounting firms and individual professional accountants carrying out business activities in accounting (Article 3(1)(8) of the AML/CFT Law) conduct CDD measures.

   AIFC members are legal firms, notary firms and other independent legal enterprises, accounting, audit and bankruptcy firms (sub-par. 19 par. 1 of Article 3 AML/CFT Law, sub-clause 5, clause 5 of the Financial Service and Ancillary Services offered by AIFC members) implement CDD measures where MVTS providers in AIFC are required to do so;

e) the Republic of Kazakhstan is not a party to the 1985 Hague Trust Convention. Such legal forms, as a the 'foreign unincorporated entity', and trusts and company service providers, and private independent entities providing family property, and other assets management services are not recognized and not prescribed in the Civil Code of the Republic of Kazakhstan and, therefore, may not be established and registered in Kazakhstan.

   However, legal advisors, independent legal advisors, independent legal professionals may serve as agents in the establishment of legal persons. In addition, certain securities market prticipants (the central depository, custodian and broker and/or dealer authorised to maintain customer accounts as

a nominee for securities, organisation registering securities transactions with the AIFC, and single operator for the nomination of securities held by government, quasi-public sector entities) may act as a nominee for securities.

The AML/CFT Law prescribes the obligation of the obliged entities to identify foreign unincorporated entities among their customers and conduct CDD measures (sub-clause 2-1), clause 3, article 5 of the AML/CFT Law).

In the AIFC, trusts and company services providers (sub-clause 7 of cl.3 and sub-clause 6 of cl.5 of the List of Financial Services and Ancillary Services offered by AIFC members subject to financial monitoring), private independent entities providing family property and other assets management services (sub-clauses 7, clause 5 of the List of Financial Services and Ancillary Services offered by AIFC members subject to financial monitoring) are held and deemed. Those are the obliged entities. For these categories, CDD measures are to be implemented with the objective of identifying the client and any person acting on behalf of a client and any BO (sub-clause (a), (a-a) clause 6.3.1, section 6 of AIFC-FR0008) where the client undertakes occasional transactions or related transactions (at that or later time) individually or collectively valued at or above USD 15,000; and towards: (i) each client classified as a high-risk client; (ii) business relations and transactions with persons originating from countries carrying high geographical risks (sub-clauses 6.1.1., section 6 of AIFC-FR0008).

1630. **Criterion 22.2** – The shortfalls in criterion 22.1 (a) P.22 to some extent affect the performance of data storage obligations by a DNFBP person.

1631. Pursuant to clause 4, article 11 of the AML/CFT Law, DNFBP persons, retain during a minimum 5-year period all requisite information obtained as part of CDD both regarding business relations and one-off transactions with a client to enable the DNFBP in AIFC to keep all the records during a minimum 6-year period from the relevant notification or reporting date, and the business relationship termination date or the transaction completion date, depending whichever occurs last (sub-clause 14.5.1, section 14 of AIFC-FR0008).

1632. Clause 4, article 11 of the AML/CFT Law places the requirement for potential recovery of the aforementioned data but without laying down the provision for such restored data to be used for criminal prosecution purposes. However the provisions of the Criminal Procedure Code of the Republic of Kazakhstan (article 111, article 112, article 118, article 120 and article 122) impose no restriction on inquiry bodies, inquiry officers, investigators, prosecutors, and courts of law to use DNFBP information as evidence.

1633. According to sub-clause 3, clause 1, article 12-2 of the AML/CFT Law, charitable entities and religious association are required to retain for a minimum five year period any information on transactions undertaken with money and (or) other property subject to mandatory state registration and on founders (members).

1634. **Criterion 22.3** – The obligation to select public officers, and their family members from among clients (beneficial owners) and apply CDD measures towards them is enshrined in articles 5 and 8 of the AML/CFT Law.

1635. The term ‘Public Officer’ for the national category of public officers within the meaning of clause 3-1), article 1 of the AML/CFT Law includes:

- an individual holding a respective public office;
- an office holder;
- an individual charged with performing public functions;
- an individual performing administrative functions at a public organization or quasi-public sector entity.

1636. These terms are defined in article 1 of the Law of the Republic of Kazakhstan 410-V (subclauses 1-1, 2, 3). The Chairperson of the Supreme Court and political party leaders appear to be excluded from the list.

1637. Since there are no special features of implementing measure towards national and foreign PEP persons in the national law and the AIFC law while relevant uniform rules apply to PEP persons in case of obliged entities. However certain shortcomings in R.12 (individual categories are not attributed to national PEP persons) and sub-criteria 22.1 (a, c) in R.22 can affect the performance of obligations by obliged entities towards PEP persons.

1638. Under the framework of business relations, AIFC-FR0008 makes provision for risk assessment studies, as well as procedures of identification, verification, and due diligence of clients and beneficial owners to classify PEP persons run by AIFC members. The term PEP as defined in the AIFC Special Term Glossary encompasses all position categories designated by the FATF

1639. Criterion 22.4 (met) – All DNFBP categories are required to develop internal control programs related to ML/TF risks, where the risk of using services for criminal purposes, including the risk of benefiting from technology advancements, and to carry out the risk assessment pending the launch of new products/technologies (Chapter 3 of the ICR Requirements for the Gambling Business and Raffles, Chapter 3 of the ICR Requirements for the Non-financial Sector and Chapter 3 of the ICR Requirements for Notaries Public). Internal control rules of all DNFBP categories reviewed by experts contained detailed procedures for identifying and reducing applicable ML/TF risks related to the use of new developing technologies.

1640. **Criterion 22.5**– The DNFBP has no legal grounds for relying on CDD measures implemented by a third party (clause 6, article 5 of the AML/CFT Law). However clause 8), article 5 of the AML/CFT Law allows all categories of obliged entities to empower other persons, including financial monitoring entities, to take measures to record data required for identifying an individual, a legal entity, a foreign unincorporated entity, and a beneficial owner when figuring out the intended goal and the nature of business relations (sub-clause 1), 2), 2-1), 2-2) and 4) clause 3, article 5 of the AML/CFT Law).

1641. The shortfalls in sub-criterion 22.1 (a) can affect the performance of obligations by obliged entities to exercise the right to empower other persons to implement individual components of CDD measures.

1642. AIFC members, i.e. DNFBP persons are allowed to empower a third-party to carry out CDD (section 9 AIFC-FR0008). If an AIFC member, i.e. a DNFBP person expects a third party to carry out CDD, it must take into account geographical risks (sub-clause 9.1.4, section 9 of AIFC-FR0008) and it must do it in a contingency when it immediately receives adequate and sufficient information, including when requested, on CDD measures, where a third-party person, i.e. a FI-regulated obliged entity is a member of the obliged entities group (sub-clause 9.1.1-9.1.4Б section 9 of AIFC-FR0008).

Weighting and Conclusion

1643. Deficiencies under R.10 and R.12 are applicable to DNFBPs. Certain shortfalls are identified with regards to the casino business (there are no regulations ensuring that any information obtained at CDD matches relevant details of a specific client transaction); there are no obligations binding on real estate agents to implement CDD measures both to the buyer and the seller.

1644. **Recommendation 22 is rated largely compliant**

Recommendation 23 – DNFBP: Other Measures

1645. In the previous MER, the Republic of Kazakhstan was rated as ‘Non-compliant’ according to the previous Recommendation 16 due to the fact that the requirements of the AML/CFT legislation of the Republic of Kazakhstan did not apply to precious metal dealers, precious gem dealers, trusts (property (management) trusts), organizations creating and servicing legal entities, and real estate agents as well as due to the material shortfalls identified in the outdated Recommendations 13, 14 and 15.

1646. **Criterion 23.1** – Regulatory requirements for monitoring and submitting suspicious transaction reports are contained in clause 4, article 10 and article 13 of the AML/CFT Law. All DNFBP categories, including AIFC members, alongside FI institutions are bound to submit to the FMA relevant data and information on transactions subject to financial monitoring. Also, please refer to the review provided in R.20. Financial monitoring entities, i.e. DNFBP persons and, therefore, individuals & entities bound to submit information and data to the FMA, include:

a) accounting firms and individual professional accountants carrying out business activities in accounting, notaries, lawyers, legal advisors and other independent legal professionals, as well as AIFC members – legal firms, notaries or other independent legal, accounting businesses – where they are involved in transactions with money and/or other assets on behalf of a client.

   According to clause 3, article 10 of the AML/CFT Law, relevant data and information on transactions subject to financial monitoring are not provided by: i) attorneys at law, legal advisers and other independent legal professionals where these data and information are obtained as a result of providing legal assistance in representing and protecting individuals and (or) legal entities at inquiry bodies, preliminary investigation authorities, and courts of law, as well as providing legal assistance in the form of consultations, explanations, counseling and written opinions on issues requiring professional legal expertise, filing legal claims, complaints and other legal documents; ii) notaries public as part of performing notary acts not involving money and (or) other property and as part of providing legal assistance in the form of consultations, explanations, counseling and written opinions on issues requiring professional legal expertise;

b) individual entrepreneur (sole traders) and legal entities undertaking transactions involving precious metals and gems and associated jewelry items as well as AIFC members, i.e. precious metals and gems dealers (no transaction threshold value is set) and dealers of any item on sale priced at or above USD 15,000.

   This DNFBP category that is not deemed to include AIFC members is subject to financial transaction monitoring where (sub-clause 1) and 2), clause 1, article 4 of the AML/CFT Law: i) pawn shops undertake a one-time transaction for the amount equal to or above KZT 3,000,000 (equivalent to around USD 6,200) in cash and non-cash form and any other categories of financial monitoring entities when precious metals and gems and associated jewelry items sold and purchased at the amount equal to and above KZT 5,000,000 (equivalent to about USD 10,500) in cash form, which in both cases does not exceed the FATF stipulated threshold of USD 15,000; ii) when any other categories of financial monitoring entities undertake transactions involving precious metals and gems and associated jewelry items sold and purchased at the amount equal to and above KZT 5,000,000 (equivalent to about USD 10,500) in cash form as well as a one-time transaction for the amount of KZT 500,000 (USD one thousand).

c) As indicated in the analysis of cr.22.1, some functions of the TCSPs are assigned to legal advisors, independent legal professionals, and certain securities market participants, as well as AIFC members. They are required to send STRs in relation to suspicious transactions as they are obliged entities (sub-clause 2-1, clause 3, article 5 of the AML/CFT Law, sub-clauses 13.7.2, 13.7.3, 13.6.1.(d) and 13.8.1 of AIFC-FR0008).

1647. **Criterion 23.2**– Requirements for internal control arrangements within DNFBP referenced in criterion 23.1 are laid down by the AML/CFT Law (article 11) and AIFC-FR0008. The ICR rules must include:

- internal control programs requiring the appointment of an officer in charge of implementing and enforcing internal control rules from among the obliged entities management or other key personnel place at or above the level of a business unit leader and other requirements placed on financial monitoring personnel responsible for implementing and enforcing internal control rules, including the impeccable business reputation (paragraph 2, part 3, article 11 of the AML/CFT Law).

These requirements of the AML/CFT Law are detailed in the ICR Requirements for the non-financial sector (sub-clause 9-11). Clause 6 of the ICR Requirements states regarding notaries public that they are officers in charge of setting up and enforcing ICR rules.

DNFBPs in AIFC are required to appoint an officer in charge of AML and provide him/her with respective responsibilities (clause 13 of AIFC-FR0008);

- AML/CFT training and education programs for obliged entities. ICR Requirements for all DNFBP categories, including AIFC members, contain provisions on training programs.

1648. The requirements for the ICR of DNFBPs – obliged entities include obligations for the internal audit function or other body authorized to perform internal audits to assess the effectiveness of internal controls for AML/CFT purposes. The functions of the obliged entities related to the organization of internal control should not be combined with the functions of the internal audit service or other body authorized to carry out internal audit (clauses 3, 9, 13 of the IRC for the non-financial sector, clauses 6, 11, 14 for notaries, clause 6, 11, 16 for organisers of gambling industry).

1649. DNFBP – AIFC members are statutorily required to develop audit rules to enhance internal control over financial monitoring entities for AML/CFT purposes (sub-section 14.6 of AIFC-FR0008). The auditing process may be conducted by means of internal audit or independent audit (section 'Audit Guidance', sub-section 14.6 of AIFC-FR0008).

1650. **Criterion 23.3** – The AML/CFT Law does not require the obliged entities referred to in criterion 23.1, to review transactions and implement EDD measures towards members registered (domiciled) in the country (territory) that fail to comply and (or) inadequately comply with applicable FATF recommendations or for settlement purposes, use is made of accounts in a bank registered in such country (territory) (sub-clause 4), clause 4, article 4, part 10, article 5 of the AML/CFT Law). The respective list of countries is made and posted on its website by the FMA. The ICR requirements for all DNFBP categories, including AIFC members, include the obligation to review client transactions based on sub-clause 4), clause 4, article 4 of the AML/CFT Law.

1651. The deficiency referred to in criterion 19.2 is applicable to DNFBPs in relation to the recommendation, rather than the obligation to take action regardless of FATF calls.

1652. **Criterion 23.4**– When internal control is exercised by DNFBP persons, including the AIFC members, referred to in criterion 23.1, their employees and officers are protected by clause 6 and 7, article 11 of the AML/CFT Law, sub-clause 13.7.3, clause 13 of the AIFC ANL Rules, from the liability stipulated by the applicable laws of the Republic of Kazakhstan and the respective civil contract for submitting to the FMA the information, data and documents specified by the AML/CFT Law.

1653. The requirement compelling financial monitoring entities and their personnel to refrain from releasing to any clients or other persons any details of information, data and documents submitted to the FMA on such clients and transactions undertaken by them is set in place in clause 7, article 11 of the AML/CFT Law. The ICR requirements for all DNFBP categories, including AIFC members in the exercise of their functions are included in sub-clause 12, clause 12 of the ICR Requirements for notaries public, and sub-clause 13, clause 12 of the ICR Requirements for the non-financial sector. The detailed ban on informing clients of any AML/CFT measures taken against them is contained in clause 13 of the Disclosure Guidance of AIFC-FR0008.

Weighting and Conclusion

1654. The STR requirements are legally established. Some shortfalls are highlighted in connection with compliance with the requirements of R. 19.

1655. **Recommendation 23 is rated largely compliant**

Recommendation 24 – Transparency and beneficial ownership of legal persons

1656. In the previous MER, the Republic of Kazakhstan was rated as 'Non-compliant' according to the outdated Recommendation 33 due to i) the absence of the beneficial owner definition; ii) the lack of applicable legal requirements for requesting and recording information on BOs; iii) the unavailability of updated and reliable information on legal entity BOs to competent authorities.

1657. **Criterion 24.1** – Profit and nonprofit organizations are allowed to be set up in the Republic of Kazakhstan. Paragraph 2, chapter 2 of the Civil Code of the Republic of Kazakhstan provides for a variety of legal entity types and forms in the Republic of Kazakhstan (articles 33-34 of the Civil Code of Republic of Kazakhstan); respective founders' rights in and to the property vested in legal entities incorporated by them (article 35 of the Civil Code of the Republic of Kazakhstan), their bodies (article 36 of the Civil Code of the Republic of Kazakhstan) and the main features (for example, article 41 on constituent features of legal entities). Law of the Republic of Kazakhstan 2198 provides a basic set of information to be issued to legal entities upon their incorporation (articles 6-1, 6-2, and 6-3). Law of the Republic of Kazakhstan 2198 describes in detail the process of incorporating legal entities in Kazakhstan, receiving and maintaining baseline information on incorporated legal entities.

1658. The national legislation includes relevant statutory provisions for incorporating and registering AIFC members, and sets out relevant requirements for legal entities and procedure for accrediting them as the Center's members, as well as activities, licensing procedure, applicable requirements, and legal forms (the AIFC Regulation 'On Companies').

1659. There is a statutory concept of BO (sub-clause 3, article 1 of the AML/CFT Law, (article 179-1 of the AIFC Regulation 'On Companies').

1660. **Criterion 24.2** – While the national legislation sets in place the obligation to carry out a legal entity risk exposure assessment, the public version of the National AML/CFT Risk Assessment contains no detailed and comprehensive review of such risks and vulnerabilities. The assessment contained in the Report on vulnerabilities of legal entities being involved into ML/TF schemes (approved at the MBC meeting on AML/CFT matters in May 2022) is not complete.

1661. **Criterion 24.3** – All legal entities created in the Republic of Kazakhstan are to be incorporated, regardless of their corporate purposes, business type and nature, members' composition (article 3 of Law of the Republic of Kazakhstan 2198). Any details on incorporated legal entities (branch and representative offices) are contained in the SDLP.

1662. Publicly available information includes: i) the last name, the first name and the middle name (if it is included in a personal identification document) or the name of an individual entrepreneur (sole trader); ii) the name and registration date of a legal entity; iii) the identification number; iv) the legal address (place of business); v) a business activity; vi) the CEO's last name, first name and middle name (if it is included in a personal identification document). These corporate data include the following information: the BIN; the address; the country of incorporation; the license number and type, the incorporation date and a permitted activity; the CEO's name, a shareholder's CEO; the share capital amount (for private companies, public companies and special-purpose companies) (clause 13, article 28 of the Commercial Code the Republic of Kazakhstan).

1663. **Criterion 24.4** – The Kazakh law sets in place the obligation to keep records pertaining to a company's business throughout its period of operations at the executive body's location or any other place specified in its corporate charter (clause 1, article 80 Law of the Republic of Kazakhstan 415-II, sections 52 and 55 of AIFC Companies Regulations; 2.4.1; 2.4.2 of AIFC General Partnership Rules; Rule 2.6.1; & 2.6.2; 16(3-1); (4) AIFC Limited Liability Partnership Rules; Section 25, and AIFC NPIO Regulations; Clause 25 AIFC NPIO Regulations.

1664. **Criterion 24.5** – Respective changes to incorporation details of legal entities (their branch and representative offices) are made on the basis of article 14-1 and 14-2 of Law of the Republic of Kazakhstan 2198 (by authorization and notification, respectively). Details on changes are submitted within a monthly period. Changes are recorded within a three-day period. Any existing judicial acts or orders (injunctions or

writs of attachment) issued by court officials or law enforcement officers and also the cases when a legal entity is defunct; the CEO or founder are executive managers or founders of defunct entities or listed as entities or persons involved in TF/PF activities, or invalid or lost documents are filed, are the basis for issuing an electronic notice without any action taken and informing the applicant accordingly. It is a business entity that is liable for failure to make respective changes (article 457 of the Code of Administrative Offenses, a fine of 10 to 30 minimum wage amounts (USD 68-214).

1665. Where an AIFC member's relevant incorporation details are changed, it must advise the Registrar of changes in paper form or via the dedicated online web portal (digitalresident.kz) within 14 days of the effective date of such changes. Should there be a delay in notifying the registrar of relevant changes made to registration details, the culprit member may be fined to the extent fixed by AIFC regulations. Upon submission of a relevant documentation package and payment made for post-incorporation service, a notice of updated data is given to the Ministry of Justice to file such details with the National Database of Legal Entities. The entire process of post-incorporation is conducted within 5 business days of receipt of the final documentation package by the AFSA (joint order by the Justice Minister of the Republic of Kazakhstan No. 1362 dated October 31, 2017 and the AIFC Managing Director No. 24 dated October 26, 2017 'On Approval of the Temporary Procedure for Submitting Information on AIFC Bodies & Organic Structures and the Center's Members into the National Register of Identification Numbers and Assigning Identification Numbers to the Same').

1666. While the incorporation process and post-incorporation acts are in progress, all involved individual and legal entities, including directors, CEO officers, shareholders and beneficial owner, are subject to multi-layered inspections. In particular, the registrar check compliance with AML/CFT, anti-corruption and related regulations.

1667. The norms and procedures requiring that necessary details on AIFC members are prescribed in the Order of AIFC . №AFSA-O-OA-2019-0102/1 dated 24.05.2019 «On approval of registration forms ».

1668. Criterion 24.6 (met) – A legal entity is bound to take reasonable measures to identify their BOs and record relevant details required for their identification in a specified form (article 12-3 of the AML/CFT Law).

a) A legal entity is bound to verify relevant details required for their BOs at least once per year or in the event when changes are made and also document such details; retain the same for a minimum five-year period from the date of receipt of information on their BOs and measures taken to identify their BOs.

b) A legal entity is entitled to request from their founders (members) and persons that otherwise a control legal entity and a foreign unincorporated entity any information required for identifying their BOs and updating details on the same.

   An individual, a legal entity being the founder (a member) and otherwise controlling a legal entity and a foreign unincorporated entity are bound to provide to such legal entity any information and documents required for identifying their BOs and updating details on the same.

   Relevant information and documents on BOs are submitted by a legal entity and a foreign unincorporated entity when requested by a competent authority in the manner and within the time specified by a competent authority.

c) Submission of relevant information, data and documents to a competent authority by a legal entity for the purposes and in the manner set out in the AML/CFT Law is not deemed to be either disclosure of proprietary, trade and other legally protected secrecy other than bank secrecy, or a breach in the terms and conditions of collecting and processing personal data and other legally protected information.

   Relevant information on BOs is included in the SDLP upon incorporation, but such information is not publicly available. It is provided only to competent governmental authorities (article 11 of the

Law of the Republic of Kazakhstan on National Identification Numbers). The registering authority is not obliged to verify the data entered in the SDLP to ensure that the person named by the applicant is the real BO of the legal entity.

Following recommendations given to law enforcement and special-purpose governmental authorities, they request information from business entities themselves, obliged entities and from the SDLP and identify the respective BO based on information obtained.

1669. **Criterion 24.7** – A legal person and a foreign unincorporated entity shall take available measures to identify their BOs and record the information required to identify them. A legal person and a foreign unincorporated entity must verify the accuracy of the information required to identify their BOs, update this information at least once a year or in case of changes, as well as record such information (Article 12-3(1-2) of the AML/CFT Law).

1670. Nevertheless, the BO information in SDLP is not a part of the list of the legal entity's data which shall be updated when amended or supplemented, in accordance with Article 14-2 of the Law "On State Registration of Legal Entities and Record Registration of Branches and Representative Offices".

1671. **Criterion 24.8** – Respective requirements for submitting information on beneficial owners to authorities are enshrined in article 12-3 of the AML/CFT Law.

a) The client is required to submit information on its beneficial owner upon request from obliged entities (clause 5, article 5 of the AML/CFT Law).

   According to the FI ICR requirements, the obliged entities identification program must set out a procedure for beneficial owner identification and a beneficial owner' data verification (clause 22 of the ICR Requirements for Banks and National Post Service Operator; clause 27 of the ICR Requirements for Entities Undertaking Individual Banking Transactions; clause 26 of the ICR Requirements for Insurance Entities, clause 27 of the ICR Requirements for the Unified Accumulation Fund and Pension Savings Funds; clause 26 of the ICR Requirements for Payment Institutions; clause 26 of the ICR Requirements for the Stock Exchange; clause 29 of the ICR Requirements for Securities Market participants and the Central Securities Depository; clause 16 of the ICR Requirements for the Commodities Exchange, clause 25 of the ICR Requirements for Entities Undertaking Individual Banking Transactions and Entities Undertaking Microfinance Activities, clause 27 of the ICR Requirements for Post Service Operators, clause 22 of the ICR Requirements for AIFC Members, clause 24 of the ICR Requirements for the Non-Finance Sector (Including Unlicensed Leasing Activities), clause 25 of the ICR Requirements for Notaries Public, clause 27 of the ICR Requirements for organisers of gambling industry, and clause 24 of the ICR Requirements for Virtual Asset Service Providers).

b) The national legal framework has established relevant requirements according to which a DNFBP must report to competent authorities and is authorized by a company to submit all primary information on beneficial owners and assist authorities in any other manner (the authorities to receive accounting data available to the FI, DNFBP and individuals or legal entities are detailed in part 5, article 34, part 2, article 122 of the Criminal Procedure Code of the Republic of Kazakhstan, and article 3 of the AML/CFT Law).

c) The country has provided no information on similar measures.

1672. **Criterion 24.9** – Documents and data obtained from CDD findings, including its case file, its account details (for banks and entities opening and managing accounts), and client communications are to be retained by financial monitoring entities for a minimum five year period from the date of termination of business relations with such client. Documents and information on transactions involving money and (or) other property subject to financial monitoring and on suspicious transactions as well as findings resulting from the review of all complex, major and other unusual transactions are to be retained by financial monitoring entities for a minimum five year period (clause 4, article 11 of the AML/CFT Law and 179-12

(5) of the AIFC Companies Regulations).

1673. A legal entity is bound to retain for a minimum five year period from the date of receipt relevant information on their BOs and on measures taken to identify their BOs (sub-clause 3, clause 2, article 12-3 of the AML/CFT Law).

1674. The retention periods for documents on core business and headcount are established by law (on a permanent basis or for a minimum five-year period; while the corporate charter and constituent documents, government registration documents or de-registration documents are retained for 15 years). Upon winding up, documents are transferred by the liquidation committee from the liquidated entity's archive fund to the respective national archive (clauses 12, 16 (sub-clause 8), 23-26, sub-clause 1.4 (the organizational framework for management) of the List of Typical Documents Generated in the Process of Public and Non-Public Institutions detailing the retention period as approved by MKS IO Order No. 263 dated September, 2017).

1675. **Criterion 24.10** – Law enforcement authorities may request information from a business entity, receive and use information from other entities, including national revenue authorities subject to compliance with confidentiality of trade, banking and other legally protected secrecy (article 8, 11 of the Law of the Republic of Kazakhstan 154-XIII, article 30 if the Tax Code of the Republic of Kazakhstan, article 50 of the Law of the Republic of Kazakhstan 2444, article 43 of the Law of the Republic of Kazakhstan 461-II, article 21 of the Law the Republic of Kazakhstan 56-V, and article 830 of the Civil Code of the Republic of Kazakhstan). In the course of pre-trial investigation proceedings, criminal prosecution bodies may request from individuals, legal entities and officers to submit documents and objects of material importance to the case (article 122 of the Criminal Procedure Code of the Republic of Kazakhstan). Courts are authorized to receive requisite information when criminal cases are under review (part 6, article 53, part 3, article 56, and article 362 of the Criminal Procedure Code of the Republic of Kazakhstan).

1676. Also, law enforcement authorities and FMA have access to the 'LESA IES' via which information is available from other systems in place with governmental authorities, including the SDLP (cl.20 «The rules of using LESA IES» dated 31.12.2015 # 12786[65]). The access is available 24/7 (cl.38 of the Rules). The supervisory authorities have access to the SDLP through their own information systems.

1677. Pursuant to clause 2.4 of the AIFC Rules for Collaboration and Information Sharing dated December 02, 2018, when looking into the validity of the Committee's request, the AIFC may attribute its intended use for purposes of actual or potential criminal, civil or administrative enforcement proceedings arising from a legal breach in the delivery of financial services conducted by the requesting body. However this norm does not give any clue as to which criteria are applied to determine the validity of the request, under whose authority it falls and what consequences are of qualifying the request as invalid.

1678. **Criterion 24.11** – Pursuant to article 129, the Civil Code of the Republic of Kazakhstan, securities can be registered, bearer and order ones. However shares, bonds and bank certificates of deposit are exclusively registered ones. For the purpose of government regulation, control and supervision over securities & other financial instruments market players, a competent authority carries out monitoring of non-government issuers of issue-grade securities (sub-clause 1-1, article 12 of Law of the Republic of Kazakhstan 474-P).

1679. Transactions involving issue-grade securities are subject to registration with the nominee holding accounting system and the registers system for securities in the manner and within the time stipulated in a competent authority's regulatory instruments. Regarding transactions involving securities, ICR measures are implemented according to the AML/CFT Law (clause 1, article 36 of Law of the Public of Kazakhstan 461-P).

[65] No longer valid as per the Order of the Prosecutor General of the Republic of Kazakhstan dated on 13.01.2023 #21

a) A bearer security is defined as one of the forms of securities issue in the Civil Code of the Republic of Kazakhstan; however the national legislation on the securities market, joint stock companies, investment and venture capital funds makes no provision for issue of bear securities.

b) The national legal framework makes no provision for converting bearer shares and bear warrants into registered shares and warrants.

c) The national legal framework contains no provisions on potential immobilization of bear shares and bearer warrants by placing the requirement that they are to be retained in a FI or with a professional intermediary.

d) The country's securities market legislation obliges issuers and investors with a controlling interest to disclose information (Articles 102 and 105 of Law-461-II).

e) The country has provided no information on other legal arrangements.

1680. **Criterion 24.12**

a) Even though there are certain legal arrangements for disclosing nominators (for example, in the course of an inspection conducted by a competent authority) in the legislation of the Republic of Kazakhstan, nominee shareholders and directors are not required by any provisions to disclose to a company and any respective registrar the identity of their nominators and to include such information into a respective register. Also, the absence of legal provisions on liability for using nominee directors casts some doubt on the adequacy of legal regulation.

b) The national legal framework places no requirements on nominee shareholders and directors to hold any license, to have their nominal status recorded in companies' registers, to retain information identifying their nominator and grant competent authorities access to such information when requested.

c) The country has provided no information on any other available legal arrangements.

1681. **Criterion 24.13** – Legal entities are held liable for non-compliance with applicable laws and regulations of the Republic of Kazakhstan on anti-money laundering and terrorist financing in the manner set out in article 214 of the Administrative Offense Code, however it does not imply that it covers failures to update and retain primary information on beneficial owners.

1682. **Criterion 24.14** – Article 19-1 of the AML/CFT Law regulates international collaboration in the area of AML/CFT.

a) The law enforcement authorities of the Republic of Kazakhstan are empowered to request upon inquiry from a foreign law enforcement body any information, including primary information retained in the companies' register (articles 19-1 and 19-4 of the AML/CFT Law).

b) The law enforcement authorities of the Republic of Kazakhstan are empowered to request upon inquiry from a foreign law enforcement body any information, including details on shareholders.

c) Public authorities (the FIU, law enforcement, special-purpose governmental authorities, and supervisory bodies) are empowered to obtain information on legal entities, including data required for international collaboration.

1683. **Criterion 24.15** – According to information provided by the Republic of Kazakhstan, the FMA maintains on an ongoing basis statistical records of any information submitted/obtained as part of the Egmont; however the country has provided no information on respective legal regulations. In accordance with the Order No. 290 dated 28 September 2021 "On Introduction of Monitoring and Quality Assessment of Information Received in the Framework of International AML/CFT Cooperation", ARDFM monitors and assesses the quality of information received in response to its requests on international cooperation in the field of AML/CTF/CPF, including information on beneficial ownership. There is no available information on other authorities.

Weighting and Conclusion

1684. Currently, the legal framework of the Republic of Kazakhstan contains a raft of regulations on incorporation of legal entities and requirements for founders and other members of business entities; sets in place the term 'beneficial owner' and provisions on requesting and registering information on BOs and granting competent authorities access to the same. At the same time, the legal entity risk assessment carried out is not complete and comprehensive, the data on the BOs in SDLP is not verified, there are no provision on updating the information in SDLP on a regular basis and corresponding liability for failure to meet most of criteria included in the recommendation.

1685. There are no provisions for requiring nominee shareholders and directors to disclose and include information in the relevant register. No liability for the use of nominee directors has been established. In addition, there are no requirements for nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, for them to keep information identifying their nominator, and for this information to be available to competent authorities upon request.

1686. There are no regulations (except for ARDFM) on monitoring the quality of assistance from other countries in response to requests for basic and beneficial ownership information, or tracing of BOs abroad.

1687. **Recommendation 24 is rated partially compliant.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

1688. In the previous MER, the Republic of Kazakhstan was rated as Non-Compliant according to the outdated Recommendation 34.

1689. **Criterion 25.1**– Kazakhstan is not contracting party of the Hague Convention on the Law Applicable to Trusts and on their Recognition of 1 July 1985. There are no legal requirements for the operation of trusts in Kazakhstan, with the exception of the AIFC premises. Therefore, criteria 25.1a and 25.1b apply to the AIFC only, and 25.1c applies to both the AIFC and Kazakhstan territory outside the AIFC. At the same time, the Chapter 30 of the Tax Code of the Republic of Kazakhstan and AML/CFT Law provides for the concept of a "foreign unincorporated entity", which is recognized as a customer of the obliged entities and among which the trust is included.

a) A trustee of an express trust must at any time take reasonable steps to obtain, maintain and record adequate, accurate and current information on ultimate beneficial owners (the UBO) concerning UBOs of any party to a trust, including the founder, the administrator, the protector, beneficiaries, any other agents and any individual providing ultimate and effective control over a trust (Section 56 (6) (a)) of the AIFC Act on Trust Regulation dated August 6, 2019 and at any time to take reasonable step to obtain, maintain and record adequate, accurate and current information on UBO (Section 56(6)(b)). However, the term 'reasonable steps' is not evaluative and provides no insight as to whether a trustee of an express trust has put in sufficient requirements to efforts when performing his /her acts.

   Due to the lack of legislation on legal arrangements the sub-criterion a) is not applicable to the territory outside the AIFC.

b) A trustee of an express trust must keep records of names and agents and service providers being points of contact that are engaged on behalf of a trust (Section 56(6)c). However, this does not directly refer to investment advisors or managers, accountants, and tax advisors.

   Any information on each party to a Trust, being an individual, includes the full legal name, residence address, the date and place of birth, citizenship, relevant personal identity documents details, the date when such individual has become a UBO and the date when such individual has ceased to be a UBO. (Section 56(11)).

Due to the lack of legislation on legal arrangements the sub-criterion b) is not applicable to the territory outside the AIFC.

c) Any information consistent with section 56(6)(a) and (b) must be retained during a six-year period when it becomes invalid or irrelevant to a trust (56 (6) a) of AIFC Trust regulations AIFC Regulation No. 31 of 2019).

According to clauses 7 and 9 of Appendix 1 to the General Rules of the AIFC, provision of trust services and acting as a fund's trustee are deemed to be a regulated activity that requires to be licensed.

There are no such legal requirements for trustees of foreign unincorporated entity outside the AIFC.

1690. **Criterion 25.2** – A trustee of an express trust must at any time take reasonable steps to obtain, maintain and record adequate, accurate and current information on ultimate beneficial owners (the UBO) concerning UBOs of any party to a trust, including the founder, the administrator, the protector, beneficiaries, any other agents and any individual providing ultimate and effective control over a trust (Section 56 (6) (a)) of the AIFC Act on Trust Regulation dated August 6, 2019 and at any time to take reasonable step to obtain, maintain and record adequate, accurate and current information on UBO (Section 56(6)(b)). However, the term 'reasonable steps' is not evaluative and provides no insight as to whether a trustee of an express trust has put in sufficient requirements to efforts when performing his /her acts.

1691. According to clause 5 of the AML/CFT Law, all obliged entities, including those being the target audience of this recommendation, carry out CDD for their clients. Information is updated where there are some reasons for doubts over previously obtained data on the client, and the beneficial owner and where required by applicable internal control rules.

1692. There are no such legal requirements for trustees of foreign unincorporated entity outside the AIFC.

1693. **Criterion 25.3**– An obliged entity is entitled to request from the customer (its representative) to make available information and documents required for identifying the customer (its representative) and establishing who a BO is and submitting relevant details on tax residency, business nature and the source of funding for ongoing transactions (clause 5 of the AML/CFT Law). However these legal norms imply that trust protectors are meant.

1694. Customers (and their representatives) must submit information and documents to obliged entities enabling them to perform their obligations set out in the aforementioned law, including information on BOs.

1695. **Criterion 25.4** – The legal framework of the Republic of Kazakhstan has no norms either restricting or preventing the disclosure of Information by trust founders to respective competent authorities and obliged entities.

1696. Submission to a competent authority of information, data and documents by obliged entities for the purposes and in the manner stipulated in the AML/CFT Law is not deemed to be disclosure of proprietary, trade, banking or other legally protected secrecy. Relevant information and documents on BOs are submitted by a foreign unincorporated entity when requested by a competent authority in the manner and within the time specified by a competent authority (clause 6, article 11, and clauses 5 & 6, article 12-3 of the AML/CFT Law).

1697. **Criterion 25.5** – The national legislation empowers a competent authority to request any information, data and documents on transactions involving money and (or) other property from obliged entities and from public authorities in the Republic of Kazakhstan.

1698. Also, the law provides for criminal intelligence and surveillance activities to be conducted whereby law enforcement authorities may request data and information from business entities, including obliged entities (clause 1, article 17 of the AML/CFT Law, and article 8 & article 11 of Law of the Republic of Kazakhstan 154-XIII). There are no disclosure requirements for trustees of foreign trusts operating outside

the AIFC, except for the provision of such information upon request of the FMA (Article 12-3(5) of the AML/CFT Law).

1699. In AIFC a trustee of an express trust must upon receipt of a notice issued by the AFSA submit the information referenced in sub-sections 56(6)(a) and (b) to the AFSA within the time and at the place that may be included in such notice (Section 56(6)(f)) for the following purposes: i) regulation with respect to AML/CFT issues, illegal organizations and compliance with sanctions at the AIFC and any other laws at AIFC; ii) disclosure of such information upon request from a regulator, a law enforcement authority and other governmental authorities. This provision does not apply to situations when trustees are required to submit to any obliged entities information on beneficial owners and trust assets that will be retained and managed in accordance with the terms of business relations (criterion 25.4) without giving reasonable explanation to such submission. The AFSA may receive information from any trustee (56 (7) of AIFC Trust regulations AIFC Regulation No. 31 of 2019).

1700. **Criterion 25.6**

a) Pursuant to the AML/CFT legislation, international cooperation is encouraged in the area of cooperation that gives rise to information sharing between the nation's competent authorities and foreign authorities by making and receiving requests for information related to identifying, preventing and investigating offenses and requests for establishing beneficial owners in entities (article 19 – 1 of the AML/CFT Law and section 11 of the AIFC Statement of Financial Accounting Standards).

b) The effective AML/CFT legislation includes collaboration between public authorities on respective information sharing.

c) The national legal framework enables competent authorities to use their investigation capabilities in accordance with the internal regulations to secure international legal assistance in a broad sense of the word. There are no requested submissions of information on beneficiary ownership.

1701. **Criterion 25.7**– The country has provided information only on the AIFC, according to which the AFSA may issue sanctions, i.e. a penalty, a warning, or a writ against a party defaulting on restitutions or compensations to any person; a writ against a defaulting party in conjunction with an explanatory note (report) on profits earned or unjust enrichment as a result of wrongdoings; a cease and desist order; a writ issued to a person to take remedial action to address or redress a wrongdoing or acts done as part of a wrongdoing; a writ prohibiting person from holding a position or being employed by an authorized person. Sanctions for breaches may be leveled at all persons by the AFSA.

1702. **Criteria 25.8–** Where the Trustee fails to comply with the requirements in section 56(6), the AFSA may impose a fine in its discretion in respect of such non-compliance and, if the fine is not paid within 30 days, may make an application to the Court for orders under subsection 17(2)(a)(i) (Application to and certain powers of the Court). If the Trustee fails to comply with such an order, the AFSA may make an application under subsection 51(1) (Removal of Trustee by Court or under the terms of a Trust).

1703. There are no statutory provisions on commensurate and dissuasive (criminal, civil or administrative) sanctions for failure to grant a competent authority access to the information on a trust referred to criterion 25.1.

Weighting and Conclusion

1704. There are no legal requirements for the operation of trusts and other legal arrangements, with the exception of the AIFC area. In AIFC there are determined requirements to the transparency of trusts, and appropriate measures for disclosing their status to control authorities are in place when access to relevant information of law enforcement authorities can be granted, including under the framework of international collaboration. There are vague and evaluative statements concerning obligations of officers in charge of disclosing information and timing of such disclosure. In addition, there are no legal provisions for proportionate and dissuasive sanctions (criminal, civil or administrative) for failure to provide competent

authorities with timely access to information on the trust, except for the AIFC.

1705. **Recommendation 25 is rated largely compliant.**

Recommendation 26 – Regulation and Supervision of Financial Institutions

1706. In the previous MER, the Republic of Kazakhstan was rated as 'Partially Compliant' according to the outdated Recommendation 23 due to: the lack of AML/CFT licensing, regulation and supervision over persons undertaking finance lease operations; consumer cooperatives granting their members loans; microcredit entities; pawn shops; insurance agents; persons undertaking e-money transactions; and persons collecting payments from the public; ii) the AML/CFT Law and other respective laws made no provisions for controls by competent authorities over legal compliance relating to the conduct of transactions and the suspension of transactions; iii) there was no competent authority in place to supervise the provision of financial services by KazPost AO.

1707. **Criterion 26.1** – Government control over legal compliance by FI institutions in the area of AML/CFT is exercised by respective public authorities within their purview and in the manner set out in applicable laws and regulations of the Republic of Kazakhstan (article 14 of the AML/CFT Law).

1708. Control and supervision over FIs (STBs, insurance (reinsurance) entities and insurance brokers, securities market participants, EECTBOs, EEMA, non-resident bank branches, insurance (reinsurance) non-resident entities, insurance broker non-resident branches, the KazPost) is provided by the ARDFM (clause 2-1, article 10 of the Law of the Republic of Kazakhstan 474-P, and the Presidential Decree-203 (the revision of August 31)).

1709. Control and supervision over compliance of the AML/CFT legislation by exchange offices and PSPs is carried out by the NB (clause 24-2, article 8 of the Law on the National Bank of Kazakhstan, sub-clause 28, clause 16 of the Presidential Decree-203).

1710. Control and supervision over commodities as required by the legal framework of the Republic of Kazakhstan is provided by the Protection and Development of Competition (sub-clause 68, clause 16 of the Presidential Decree-428)

1711. The FMA exercises governmental control over compliance with the AML/CFT legislation by leasing companies (sub-clause 13-5, article 16 of the AML/CFT Law).

1712. As far as AIFC members are concerned, according to article 12 of Constitutional Law of the Republic of Kazakhstan 438-V, the AFSA regulates financial services and associated activities in the Center. The AFSA provides regulation and oversight over compliance with ML/TF issues by FIs in AIFC (article 14 of the AML/CFT Law, the revision of July 28, 2022).

Market Entry

1713. **Criterion 26.2**– Institutions acting under the Core Principles (STBs, non-resident bank branches, insurance companies & insurance brokers, and securities market participants) must be licensed by a competent authority (Law of the Republic of Kazakhstan 2444, Law of the Republic of Kazakhstan 126-II, Law of the Republic of Kazakhstan 461-II, and the AIFC Framework Regulation).

1714. Other FI institutions, including FI institutions providing MVTS and money and currency exchange services, except for KazPost, must be either licensed (exchange offices) or registered (PSPs) (the Law 11-VI, the Law 56-V, the Law 105-V, the Law 167-VI, the Law 78-II, and the Law 202-V).

1715. KazPost can undertake certain types of bank operations (deposits, opening and maintaining corporate bank accounts, opening and maintaining correspondent accounts, cash operations, exchange operations, transfers) without a license.

1716. As for FIs in Kazakhstan, there is no direct ban on setting up or running shell banks, however banks and non-resident bank branches can be opened only pursuant to an authorized body's resolution subject to

compliance with legally applicable organizational and engineering requirements, including those pertaining to office accommodation & layout, equipment and management personnel (Law of the Republic of Kazakhstan 2444). Regarding the AIFC, there is a direct ban on setting up or running shell banks in the AIFC (clause 10.3 of AIFC-FR0008).

1717. **Criterion 26.3**– The requirements for preventing any criminals or their accessories/accomplices from owning a major or controlling stake in a financial institution (or a situation when they can become its beneficial owners) or from gaining their access to management functions differ for various FI categories and contain certain pitfalls.

Persons holding a major or controlling stake in a financial institution

1718. Persons without a sound business reputation are prohibited by law from being founders and holding a controlling interest in FIs, but not all the FI's supervisory authority are required to apply measures in order to prevent criminals from holding a significant or controlling interest in FIs.

1719. Respective supervisory measures exist for STBs, insurance companies, securities market participants, EECTBOs, PSPs, AIs and EEMAs, as their supervisory authorities check the business reputation of the founders and/or major shareholders when issuing a license or when registering activities, as well as when changing major shareholders.

1720. The acquisition of major shareholdings in STBs, insurance companies and securities market participants requires the prior consent of the supervisory authority, and the absence of a sound business reputation is a ground for refusing to grant such consent. Where a person acquires a significant interest in a FI without consent, the supervisory authorities may apply supervisory response measures (Article 17-1 of the Law-2444, Article 26 and 26-1 of the Law-126-II, Article 72-1 and 72-2 of the Law-461-II).

1721. For EEMA, EECTBO, PSP and AI the lack of a sound business reputation may be a reason for refusal to grant a license or registration (Art. 14 of the Law-56-V, Resolution #168 "On Approval of the Regulations on Licensing of EECTBOs" as updated on 05.09.2022, Art. 17 of the Law on Payments, Art. 19-4 Rules N°49 on the implementation of foreign exchange transactions). In case of a change of the shareholders, the EEMA, EECTBO and AI shall inform the supervisory authority no later than two weeks from the date of the change. Compliance with the business reputation will then be monitored ex post during inspections. There is no obligation to notify a change of major shareholders for the PSPs, and therefore, it is not clear how the supervisory authority monitors the business reputation in case of a change of major shareholder of PSP.

1722. There is no prescribed tool for controlling the business reputation of founders and major shareholders of Kazpost, where the sole shareholder is the Sovereign Wealth Fund "Samruk Kazyna".

1723. There are no supervisory measures in legislation to prevent criminals from owning a significant or controlling interest in insurance brokers and commodity exchanges.

1724. For the majority of FIs (STBs, insurance companies, securities market participants, EECTBO, EEMA), the sound business reputation includes the absence of unexpunged or expunged criminal record and absence from the sanctions lists. At the same time, for AIs and PSPs, the absence of a criminal record implies the absence of a criminal sanction in the form of disqualification from holding an executive position in an FI, a bank and/or insurance holding company and being a major shareholder in an FI (Article 19-1 of the Law-11-VI as updated on 01.07.2022, Article 47 of the Law-461-II, Resolution of the Board of the NB "On Approval of the Rules for Currency Exchange Transactions " as updated on in December 2021) and does not include other sanctions.

1725. The sound business reputation does not include association with criminals and, as a consequence, there are no measures and procedures in law to prevent persons associated with criminals from holding a significant or controlling interest in a FI.

1726. A "major shareholder" is defined in the legislation for insurance companies, securities market

participants, EECTBO, EEMA, as a natural or legal person owning directly or indirectly 10 percent or more of the equity or voting shares, or having control or ability to influence decisions of 10 percent or more of shares, but not as the ultimate BO of an FI. In relation to a major shareholder – legal entity, the sound business reputation shall be verified with the managing officer (Article 17-1, Paragraph 9 of the Law on banks, Article 72-2 of the Law on securities market, Article 26-1 of the Law on insurance, Article 14 of the Law on microfinance activities, Decree #168 On Approval of the Licensing Rules for EECTBO as updated on 05.09.2022). BOs of PSPs shall be checked for business reputation in accordance with the NB's Order dated on 12.09.2022. For non-banking exchange offices, the legal acts do not specify which person is subject to business reputation check in case the founder/shareholder/major shareholder is a legal entity. Consequently, there are no measures to prevent a situation where the ultimate BO of the FIs may be a criminal with the exception of the PSPs.

1727. In issuing a license, the AFSA checks business reputation of individuals holding 10 percent of shares of the FI in AIFC or above (Rule 1.1.5 (i) and Provision 1.2.5(h) of the AIFC General Rules). The criteria on which basis the AFSA reviews the suitability or fitness of persons holding a controlling stake in a FI are enshrined in the AFSA's Regulatory Guidance On Fitness and Propriety and include the background, the professional record, the core activities and the reputation of persons holding a controlling stake in the FI in AIFC, including criminal records. Where there are any doubts, the AFSA may impose licensing restrictions.

Access to Management Functions

1728. For most FIs, the legislation prescribes measures to prevent criminals from gaining access to management functions when granting a license or registration or when changing management personnel. For STBs, EECTBOs, insurance companies and brokers, securities market participants, a manager appointment should be agreed with a competent authority, and a manager must have a sound business reputation (article 20 of Law-2444, article 34 of Law-26-II, article 54 of Law-461-II, and article 55 of Law-105-V).

1729. For EEMAs, failure to comply with business reputation requirement is the basis for refusal to issue a license for undertaking microfinance activities (article 14 of Law of the Republic of Kazakhstan 56-V). Upon issue of the license, the business reputation of management personnel is checked ex post during the inspections (Order No. 526 dated December 31, 2020).

1730. For PSPs, there is also a ban on access to management functions for persons having an unexpunged or unspent conviction record, but this ban does not apply to all management functions, rather only to those of an executive body's head (article 19 of Law of the Republic of Kazakhstan 11-VI). Follow-up control is exercised when inspections are conducted.

1731. A person cannot be appointed as a manager of AI if the person is from the sanctioning list or is exposed to a valid court judgment to apply criminal punishment by disqualification from holding any management positions within a FI, a banking and (or) insurance holding company and acting as a major shareholder of a FI (article 12 of Law-167-VIthe NB's Order as updated in December 2021) Follow-up control is exercised when inspections are conducted.

1732. According to the AIFC Framework Agreement, the AFSA will not qualify an individual as suitable and fit for a managerial position, where he or she has been convicted of a grave crime, and if such individual is subject to administrative or civil judgment ((clause 43 (3) of the Framework Provisions). However, it is not clear which crimes are to be classified as a grave criminal offense, and what an administrative or civil judgment means.

1733. For commodity exchanges and KazPost, no matching provisions for denying criminals access to management are found to be in place within the regulatory framework.

Risk Based Approach to Supervision and Monitoring

1734. **Criterion 26.4**

a) Banks, insurance institutions, securities market participants and AIFC members are subject to prudential regulation and supervision, generally complying with the respective principles of the Basel Committee on Banking Supervision (BCBS), the principles of the International Association of Insurance Supervisors (IAIS) and the principles of the International Organization of Securities Commissions (IOSCO), including supervision practices applied to a consolidated group.

   The ARDFM and the AFSA are members of the IOSCO and the IAIS, and the AIFC Committee is also a member of Group of Banking Supervision Bodies from Central and Eastern Europe (the BCBS regional group).

   At the same time, the AFSA's supervision authority over AML/CFT enforcement by AIFC members acting according to the Underlying Principles, is not directly provided in AIFC regulatory instruments for regulation and supervision over these FI institutions.

   The authority of a competent body (the ARDFM) to exercise control and supervision over AML/CFT compliance does not apply to financial groups (clause 2-1, article 9 of Law-474-II). However there is a general provision on control functions exercisable by a supervision authority, including for the purposes of AML/CFT enforcement/compliance, that applies to conglomerates and holding companies (article 15-1 of Law-474-II). However there is no legal instrument covering the procedure for consolidated supervision over AML/CFT compliance.

b) Other FIs in Kazakhstan, including MVTS providers or exchange offices are subject to supervision and monitoring to ensure compliance with applicable national requirements in the area of AML/CFT Law (article 8, clause 24-2 of Law-2155, article 23 of Law-498-V, article 27 Law-56-V, article 4-2 Law-155-IV, article 14 of the AML/CFT Law , clause 13-1 and 13-2, article 16 of the AML/CFT Law).

   FI in AIFC providing MVTS as well exchange services meet applicable AML/CFT requirements, but the monitoring of these requirements is not based on the ML/TF risk.

1735. Criterion 26.5 (mostly met) – To regulate and supervise STBs, EECTBOs (including Kazpost), insurance companies, securities market participants and AIFC members, a risk-based approach is adopted (articles 3, 9, 15-1 and 15-8 of Law-474-II, sub-clause 24-2, article 8 of Law-2155, and clause 5 and clause 15 of Presidential Decree-203 and Constitutional Law of the Republic of Kazakhstan 438-V, the Framework Provisions of the AIFC, and the General Rules of the AIFC). The risk-based approach application process as part of control and supervision is deemed to be confidential information and is not to be published.

1736. For FI institutions, a risk-based approach to supervision is set out in PR-317K; PR-265K; PR-299K; and PR-300K.

1737. In formulating a risk-based approach, the FMA adheres to Joint Order of the Chairperson of the FMA #7 dated August 16, 2021 and the National Economy Minister of the Republic of Kazakhstan #80 dated August 16, 2021 'On Approval of the Risk Assessment Criteria and Checklist for Anti-Money Laundering and Terrorist Financing Compliance in the Republic of Kazakhstan.

1738. The application of the risk-based approach as part of control and supervision of legal entities' business carried on exclusively via exchange stores is set out in Procedure No. 56 (Procedure for Risk Measurement for the Purposes of Inspecting Private Business Entities by Territorial Branch Offices of the National Bank of the Republic of Kazakhstan' approved by Resolution of the Board of Directors of the NB #56 dated April 27, 2017). Regarding payment institutions, the risk assessment system building procedure is approved by Order of the Chairperson of the NB #44 dated January 24, 2019.

1739. There are no provisions on the risk-based approach applicable to commodity exchanges.

1740. Pursuant to clause 1 and clause 2, article 15-2 of Law of the Republic of Kazakhstan 474-II, a control and supervision body within its scope of authority conducts risk assessments, unscheduled and in-house

audits of target entities on a overall basis or selectively for specific business matters.

a) Regarding FIs (cl. 1 and 2 of article 15-2 of the Law-474-II) a risk assessment inspection is an inspection carried out by a competent control and supervision body within its purview by making an on-site visit to the target entity and mandated on the basis of the risk assessment of the entity to be inspected. The inspection of the target entity based on the risk assessment is conducted by a control and supervision body within its purview at least once a year.

   The list of entities to be inspected is made by a control and supervision body within its purview on a semi-annual basis based on risk assessment related to the business of entities to be inspected.

   According to approved methods, risk assessment and check-listing activities, including inspection (audit) frequency, factor in AML/CFT risks. .

   According to information provided, for FIs in AIFC, a supervision approach is based on the use of a straightforward risk assessment system to assess the risk profile of AIFC members and is configurable on the size, scale, nature and environment for each specific obliged entity and specific risks that a FI in AIFC presents for regulation and supervision purposes. FI in AIFC are subject to supervision on an ongoing basis when carrying in the AIFC business of identifying, assessing and prioritizing risks whereupon relevant decisions are taken. In addition to the right to collect information (clause 96 of the Framework Provisions), the right to request financial statements and reports (clause 97 of the Framework Provisions) and the right to conduct investigations into suspected legal violations, on April 2, 2019, the AFSA developed and approved the relevant supervision procedure (No.5/2019 (m)) for field inspections laying out key inspection processes, inspection procedure and inspection-specific documentation procedure, etc.

b) State bodies carrying out control of compliance with the legislation on AML/CFT/CPF by the obliged entities are obliged to consider the information from report of the ML/TF risk assessment while selecting the subjects (objects) of control (sub-clause 5, cl.1, article 18 of the AML/CFT Law). There are no other regulations on considering risks while determining the frequency and intensity of on-site and off-site inspections.

c) For FIs in Kazakhstan, a risk-based approach embraced as part of control and supervision is built upon the principle of proportionality allowing for the size, importance, nature, scale and complexity of FI activities and classification depending on their value in the financial market (article 15-8 of Law of the Republic of Kazakhstan 474-II).

   According to information provided, for FIs in AIFC , a supervision approach is configurable on the size, scale, nature and environment of each specific FI institution. As far as the FMA is concerned, the Order on Approval of Risk Assessment Criteria and AML/CFT Compliance Checklist in the Republic of Kazakhstan makes no allowance either for the size or specific nature of institutions.

1741. **Criterion 26.6** – The legal framework provides that a competent authority must allow for FI risks when conducting inspections (audits) (clauses 1 and 2, article 15-2 of the Law of the Republic Kazakhstan 474-II).

1742. For STBs, major shareholders of STBs, bank conglomerates, EECTBOs, EEMAs, insurance companies and securities market participants, the ML/TF Risk Exposure Assessment Procedure provides that a supervisory authority collects data on an annual basis and determines the risk assessment for FI institutions and reviews a structure of specific ML/TF risks based on high-profile events or changes in the business of an entity or a group.

1743. The risk assessment methods employed by PSPs and AIs provide for the review of a list of risk factors on an annual basis based on the business performance of FI institutions for the previous year and supervisory actions.

1744. According to submitted information, for FIs in AIFC, the AFSA has developed a method (model) of

FIs in AIFC exposure to ML/FT risk. This method includes a quantitative quality analysis and also FI rating risk measurement. This rating is reviewed on a regular basis based on remote supervision and inspection findings.

Weighting and Conclusion

1745. The Republic of Kazakhstan has put in place AML/CFT supervision and control authorities for all FI institutions and all FI institutions are to be subject to supervision and monitoring for compliance with AML/CFT requirements. The activities of all FIs (except for KazPost) are subject to licensing, registration or notification. At the same time, the legislation does not provide for all measures to prevent criminals or their associates from holding significant shares or having access to management functions in FIs. In particular, there are no requirements for checking the business reputation of the ultimate BO and a major shareholder, that is a legal entity, as well as measures and procedures preventing persons having links with criminals to own a major or controlling stake in a FI. There are no measures to check the business reputation of major shareholders and managers of commodity exchanges. There is no requirement for supervisory authorities to consider ML/TF risks prevailing in the country when applying the risk-based approach in supervision. There is no any legal regulation laying down the procedure for consolidated supervision in the AML/CFT in relation to financial groups.

1746. **Recommendation 26 is rated partially compliant.**

Recommendation 27 – Powers of supervisors

1747. In the previous MER, the Republic of Kazakhstan was rated non-compliant as supervisors basically had no powers to conduct inspections, to take enforcement measures or sanctions. Moreover, there was no practice of AML/CFT inspections of Fis.

1748. **Criterion 27.1**– Each category of FIs is legislatively supervised by the supervisory authorities (ARDFM, NB, FMA, APDC) for compliance with AML/CFT requirements (see Cr.26.1).

1749. The AFSA has powers to impose upon FIs in AIFC disciplinary sanctions, to take enforcement measures, and to take any other regulatory action for breaching the requirements of AIFC-FR0008 (para. 2.2 I).

1750. **Criterion 27.2**– Statutory provisions applicable to the powers of supervisors relating to inspections of FIs are enshrined in Law 474-II (for ARDFM and NB), in the Presidential Decree-428 (for APDC) and in the CMOC (for FMA).

1751. The supervisors may conduct monitoring, scheduled and unscheduled inspections of FIs (para. 2 of Article 9 of Law 474-II).

1752. The AIFC legislation, the Regulations on the Systemic Regulation of Financial Services regarding the powers of the AFSA (part 8 of Chapter 1 of the FSFR) do not set out any special provisions on how to conduct inspections of FIs in AIFC, with the exception of the right to collect information (para. 96 of the Framework Regulations) and the right to conduct inspections on suspicion of breaches of law, including inspections in the premises of FIs with a view to checking and copying information or documents kept in those premises.

1753. Information provided by the country suggests that the AFSA, in furtherance of the RBA, may organise ML/TF inspections of FIs in AIFC, inspections of how they comply with CDD requirements and UNSC Resolutions and sanctions. Inspections may include both interviews of personnel and management of FIs in AIFC and inspections of all their records and documentation. However, these rights are not enshrined in legislation. Nevertheless, on 3 April 2019 (No. 5/2019 (m)), the AFSA developed and approved a supervisory procedure on how to conduct on-site inspections which covers the key processes of such inspections, the procedure for conducting them, and the procedure for drafting documents during such inspections.

1754. **Criterion 27.3** – Supervisors may collect information without any restrictions and obtain any information pertaining to the functions of control and supervision over how FIs comply with the laws of the Republic of Kazakhstan, including AML/CFT (Article 17 of the AML/CFT Law, Article 14 of Law 474-II, Article 70 of Law 2155, Presidential Decree 203, Presidential Decree 1271, the Presidential Decree "On Certain Matters of the Financial Monitoring Agency of the Republic of Kazakhstan", para. 16 of the Presidential Decree "On Certain Matters of the Agency for Protection and Development of Competition", cl.8(1) of Framework Provisions of AIFC).

1755. **Criterion 27.4** – The ARDFM, NB and AFSA are authorised to apply to the supervised FIs disciplinary sanctions for non-compliance with AML/CFT requirements in accordance with the laws of the Republic of Kazakhstan (Article 9, subpara. 10 of Article 10 and Article 15-8 of Law 474-II, Presidential Decree 203, subpara. 4 of para. 15 of the Regulations of the ARDFM, subpara. 2), para. 2 of Article 22 of Law 167-VI, Article 18 and para. 1 of Article 24 of Law 11-VI, para. 8 of Article 57 of Law 2444, Article 51 and para. 8 of Article 55-1 of Law 461-II, Article 16 of Law 56-V, Articles 54 and 55 of Law 126-II, cl.2.2(c) of AIFC-FR0008 as amended 12.12.2021).

1756. Disciplinary sanctions in relation to securities market participants, EEMAs, insurance companies and AIFC members include suspension or withdrawal of license in cases of violations of the requirements of the AML/CFT Law (Law-461-II, Law-56-V, Law-126-II, Law-105-V, section 2.2 (c) AIFC-FR0008 as amended 12.12.2021 and the MFC Framework Provisions). The suspension or revocation of licences for STBs, EECTBOs and AIs is not explicitly provided for in case of non-compliance with AML/CFT requirements, but is part of the general powers of the ARDFM and NB, applicable in case of systematic violations of legislation on matters within their competence, including the supervision of compliance with AML/CFT legislation. The NB has no statutory powers to remove a PSP from the register for failure to comply with AML/CFT legislation.

1757. The APDC is not empowered by law to impose disciplinary sanctions in the form of revocation or suspension of the license of commodity exchanges for non-compliance with AML/CFT legislation.

1758. For FIs outside the AIFC, financial sanctions are imposed in accordance with article 214 of the CAO, which presents a list of penalties for breaching various requirements of the AML/CFT legislation imposed upon all obliged entities. The amount of penalties is calculated based on monthly calculation indices and varies depending on the offence. The amount of penalties is enshrined in legislation and cannot be changed by the supervisor. The supervisory authorities are not entitled to impose administrative fines themselves, but must refer the protocols for review to a court, which decides on the imposition of a fine.

1759. The AFSA may impose financial sanctions to FIs in AIFC for violations of AML/CFT requirements, including imposing such amounts of penalties for breaches upon FIs in AIFC as it deems necessary (part 8 of the FSFR, Sections 98-101; 118).

Weighting and Conclusion

1760. Supervisors are empowered to exercise supervision and monitoring over how FIs comply with the AML/CFT requirements, and may conduct inspections of FIs and demand any information, as well as to impose disciplinary sanctions on most of the supervised FIs. The lack of authority of the NB to exclude PSPs from the register and the lack of authority of the APDC to impose disciplinary sanctions on commodity exchanges for non-compliance with AML/CFT requirements present certain shortcomings. Most supervisory authorities do not have the authority to impose financial sanctions themselves, but practice shows that this does not affect the effectiveness of the imposition of fines.

1761. **R.27 is rated largely compliant.**

Recommendation 28 – Regulation and supervision of DNFBPs

1762. In the previous MER, the Republic of Kazakhstan was rated non-compliant with the former R.24 for the following reasons: i) the list of obliged entities did not cover DMPS, real estate agents, accountants,

with public notaries not covered by AML/CFT control; ii) there was no effective monitoring over how DNFBPs comply with AML/CFT measures, including sanctions; iii) there were substantial deficiencies in the legislative powers of supervisors when it comes to requesting information, and there was *de facto* no body to exercise control over how attorneys comply with the AML/CFT Law and no supervisor to exercise control over the activities of independent law specialists, and so forth.

Casinos

1763. **Criterion 28.1**

a) Casinos belong to the gambling business industry and are regulated by Law 219-III (subpara. 1) of para. 1 of Article 6).

   State regulation of the gambling business industry in the Republic of Kazakhstan takes the form, *inter alia*, of licensing (subpara. 2) of para. 2 of Article 5 of Law 219-III).

   Licenses are issued for each gambling establishment for ten years (para. 2 of Article 9 of Law 219-III).

   Electronic casinos and Internet casinos are prohibited in the territory of the Republic of Kazakhstan (subpara. 2) of para. 2 of Article 6 of Law 219-III). There are no ship-based casinos in Kazakhstan;

b) Casinos amd other organisers of gambling industry are subject to general requirements which include the founder, member or BO having no unexpunged or unspent conviction for an economic crime or deliberate medium-gravity crime, grave crimes, especially grave crimes, and cases when the founder (member) of the casino is a founder or member of a legal person that has tax arrears or is declared bankrupt (para. 16 of Article 12 of Law 219-III). Persons with an unexpunged or unspent conviction cannot manage casinos and other gambling entities (para. 17 of Article 12 of Law 219-III). There are no regulatory requirements preventing criminals or their associates (other than those mentioned above) from being the BO of a casino or other organiser of gambling industry;

c) control over how gambling organisers comply with the AML/CFT legislation is exercised by the MCS – an authorised body (subpara. 257) of the section "Functions of the Agency" of para. 16 of the Regulations on the MCS approved by Resolution No. 1003 of 23 September 2014 of the Government of the Republic of Kazakhstan).

Other categories of DNFBPs

1764. **Criterion 28.2) –** The relevant state authorities perform monitoring and control over how obliged entities comply with the AML/CFT legislation in accordance with their competence (Article 14 of the AML/CFT Law). All DNFBPs, except lawyers, are subject to supervision.

1765. There is no authority to exercise control (monitoring) over AML/CFT compliance by the lawyers. According to subpara. 10) of para. 2 Article 55 of Law 176-VI, the Council of the Bar Association organises compliance with the AML/CFT legislation which is inconsistent with the basic requirement of Article 14 of the AML/CFT Law on AML/CFT state control by the relevant state authorities in accordance with their competence, however, this does not run contrary to international standards.

1766. **Criterion 28.3**– According to para. 57 of Article 138 of the COMC, AML/CFT is applicable to the area of activity of entrepreneurs in which state regulation and control are exercised.

1767. Given the forms of control and supervision defined in Article 137 of the COMC, control and supervision, including in the AML/CFT area, are exercised as inspections and as preventive control and supervision which are proactive and preventive in nature.

1768. The AFSA exercises control and supervision of AIFC members (subpara. 5) of part 3 of Article 12 of Law 438-V). Subpara. 2.3 of AIFC-FR0008 sets out supervisory powers of the AFSA in respect of DNFBPs which state that the AFSA may conduct reviews of DNFBPs in order to comply with its AML/CFT obligations, including in furtherance of its risk-based supervision.

1769. **Criterion 28.4**

a) the area of control, including inspections and monitoring, over the activities of individuals, engaged in entrepreneurial activities, and commercial and public organisations and notaries includes compliance with the AML/CFT legislation (para. 57) of Article 138 of the COMC).

Taking into consideration the analysis of c.28.2, the powers of the state bodies and SRBs to conduct AML/CFT inspections (monitoring) of such a category of the DNFBP sector as attorneys are insufficient due to the fact that the Council of the Bar Association only arranges the compliance with AML/CFT law and is not empowered to conduct inspections.

The AFSA has powers to exercise control and supervision over AML/CFT compliance in relation to DNFBPs in AIFC (see c.28.3).

b) The Kazakh legislation sets forth a certain set of requirements for specific categories of obliged entities of the DNFBP sector that relate to denying criminals DNFBP professional accreditation in respect of:

- Attorneys, legal counsel – a person who has an unexpunged conviction or who has not spent his conviction as prescribed by law and against a relevant certificate is not allowed to engage in these activities; besides, a person is not allowed to practise law if he is released from criminal liability, dismissed from state and military service with cause, from the law enforcement, special state bodies, and is released, or committed an administrative corruption offence, has his bar license revoked, is struck off from the register of the chamber of legal counsel with cause (Law 176-VI);
- audit firms – audit licenses will be denied in the following cases: i) there is an effective court decision (judgment) in respect of the license applicant that relates to the suspension or prohibition of activities or certain types of activity that are subject to licensing; ii) as requested by the bailiff, the court temporarily prohibits one from issuing a license to the license applicant who is a debtor (para. 9 of the State Service Standard "Issuing Audit Licenses" which is an annex to the State Service Rules "Issuing Audit Licenses" approved by Order No. 336 of 30 March 2020 of the First Deputy Premier Minister – the Minister of Finance of the Republic of Kazakhstan), and, when issuing a license to an audit firm, it is necessary for the head to have confirmation that the audit firm he used to lead earlier did not have its license revoked (para. 5 of the Qualification Requirements and List of Documents Evidencing Compliance with Them for the Purposes of Audit Activities approved by Resolution No. 1434 of 12 November 2012 of the Government of the Republic of Kazakhstan) However, there is no specific guidance on the exclusion of criminals from auditing activities in legislation;
- notaries – a prohibition to engage in such activities for a person who has an unexpunged conviction or who has not spent his conviction as prescribed by law (part 4 of para. 1 of Article 6 of Law 155-I);
- requirements to the ICR for the non-financial sector (including jewellers, real estate agents), organisers of gambling industry set out that the head and senior official of obliged entities should be persons who have a sound business reputation, that means, *inter alia*, no unexpunged or unspent conviction for economic crimes, or deliberate medium-gravity crimes, grave crimes, especially grave crimes (para. 9 of the ICR Requirements for the non-financial sector; part 3 of para. 11 of the ICR Requirements for organisers of gambling industry). BOs of dealers of precious metals and stones, real estate agents, and their associates are not subject to such requirements.

Additionally, if DNFBP is managed by a legal person, registration will be denied if:

- the natural person who is the founder (member) and (or) head of the legal person has an unexpunged or unspent conviction for crimes under Articles 237 (Illegal Actions during

Rehabilitation and Bankruptcy), 238 (Deliberate Bankruptcy) of the Criminal Code of the Republic of Kazakhstan;

- during state registration/reregistration, the founder (natural and (or) legal person), its founders, head of the legal person, the founder and (or) head of the legal person that is the founder (member) of the legal person, are debtors under a writ of execution, with the exception of the person who is a debtor in enforcement proceedings relating to the recovery of periodic payments (subparas. 4-4) – 4-6) of Article 11 of Law 2198).

  However, these requirements do not apply to persons associated with the Bos of DNFBPs.

  Insofar as AIFC members are concerned, when disclosing information about ultimate BOs, irrespective of the type of activity and form of business of the member, apart from identifying BOs at the threshold level, it is necessary to identify all main BOs in order to ensure that that these are not affiliated one way or another (Article 14-1, Article 179-1 of the AIFC Act "On Companies", para. 6.1.4 (b) of the AIFC Rules on AML/CFT).

c)

- Administrative sanctions are imposed when obliged entities are found to be non-compliant with the AML/CFT requirements, with such sanctions extending to suspensions of licenses or qualification certificates. Legal persons and officials may be held administratively liable (see R.35).
- The MCS, MoJ, CIPA of the MoF are empowered to suspend, withdraw existing licenses to engage in activities and to issue instructions to remedy deficiencies. Besides, only the body that licenses the practice of law has powers to suspend licenses for six months in view of the systemic (three and more times during twelve consecutive calendar months) breaches of requirements under the AML/CFT Law (subpara. 5) of para. 1 of Article 43 of Law 176-VI;
- Additionally, obliged entities may be wound-up under Article 49 of the CIVC, CIVPC and Law 416.
- See R.15 for the analysis of sanctions against VASPs in AIFC. These sanctions are also applicable to DNFBPs in AIFC.

1770. The legislation analysis in R.35 does not make it possible to reach a conclusion on the availability of a wide range of sanctions and on the proportionality and dissuasiveness of criminal and civil law sanctions which are imposed upon obliged entities, with the exception of AIFC members that are DNFBPs and natural persons who violated the AML/CFT legislation. It is difficult to reach a conclusion on the proportionality and dissuasiveness of sanctions in respect of AIFC members given that the inspections, including the imposition of liability measures, are not completed.

All DNFBPs

1771. **Criterion 28.5**

a)-b) The COMC establishes a general risk-based supervision mechanism. The COMC provides for such types of control as: inspections, and preventive control and supervision with or without a visit paid to the subject (object) of control (Article 137). Inspections may be scheduled (these are conducted following the assessment of the risk level of the inspectee) and unscheduled (these are conducted following the discovery of specific facts about a certain subject of control (supervision) (Article 144). AML/CFT matters are covered by state control and supervision (para. 57) of Article 138 of the COMC). However, AML/CFT matters are not covered in the risk assessment of the inspectee. AML/CFT matters are addressed during comprehensive inspections established by the above general supervision mechanism.

Advocates are not covered by the COMC which implies that they are not subject to AML/CFT

risk-based supervision. However, the Council of the Bar Association is required to analyse and monitor the activities of lawyers within its competence for the detection of ML/TF risks (paras.18-12 cl. 3 of Article 68 of Law-176-VI).

There is no information to the effect that supervisors should factor into the diversity and number of supervised persons and organisations in the DNFBP sector, the degree of discretion permitted under the RBA.

The AFSA exercises AML/CFT control and supervision as part of its risk-based supervision, including ML/TF risks (para. 2.3 of AIFC-FR0008). When on-site inspections take place, the following characteristics of DNFBPs are examined in a comprehensive manner: type of activity, country of registration, services provided and channels through which services are provided, internal controls, their quality, CDD availability, transaction monitoring, awareness, internal audit, and others. The SRA and NRA results are used to determine the frequency and scope of inspections. There are no completed inspections.

Weighting and Conclusion

1772. Casino activities are licensed in the country, with heads and owners subject to relevant requirements. All categories of DNFBPs, with the exception of attorneys, have their own body attached to them that exercises AML/CFT state control and monitoring. The Council of the Bar Association ensures that advocates comply with the AML/CFT legislation. The AFSA is instructed to exercise intensive supervision of AIFC members. Persons affiliated with the Bos of DNFBPs are not identified. Not all officials of DNFBPs may be held administratively liable. Types of corrective actions are not sufficiently diverse, consequently lacking deterrence. Risk-based supervision of the DNFBP sector does not take into account the type and number of DNFBPs, the ML/TF risk profile. The sanctions imposed on AIFC members are to prevent criminals and their accomplices from owning the organisation or obtaining accreditation, active oversight by the AFSA, the range of sanctions measures is varied.

1773. **R.28 is rated partially compliant.**

Recommendation 29 – Financial Intelligence Units

1774. In the previous MER (June 2011), the Republic of Kazakhstan was rated largely compliant with the former R.26. The first round of the MER revealed the following deficiencies: the scope and procedure of powers (rights and obligations) delegated to the FIU within the limits of competence of the MoF needed clarification and better regulation; the scope of powers of the Chairman of the FIU raised questions regarding the operational independence of the FIU; reports published about the FIU performance did not contain the basic statistical figures, identified typologies and trends; inaccuracies in the wording of legislative acts (as far as information exchange with foreign FIUs is concerned) and abuses in the implementation of recommendations of the Constitutional Council may lead to what FATF and the Egmont Group believe to be unreasonable refusals to execute requests forwarded by other FIUs.

1775. **Criterion 29.1** – The FMA administers AML/CFT matters (para. 1 of the Regulations on the FMA approved by Presidential Decree 515 of 20 February 2021) and collects, processes and analyses information about funds and (or) other property subject to financial monitoring, sending afterwards the results of such analysis to the LEAs and special state bodies of the Republic of Kazakhstan (Articles 15-16 of the AML/CFT Law, para. 16 of the Regulations on the FMA approved by Presidential Decree 515 of 20 February 2021).

1776. Financial monitoring is also performed in relation to suspicious transactions which include ML/TF and other criminal activities (para. 1 of Article 1 of the AML/CFT Law).

1777. **Criterion 29.2**

a) the FMA collects and processes information about funds and (or) other property subject to financial monitoring (para. 1 of Article 4 and Article 10 of the AML/CFT Law, para. 1 of Presidential Decree 13).

   Data and information about transactions subject to financial monitoring are forwarded to the FMA by electronic means using approved forms (para. 2-3 of Presidential Decree 13).

   Further, the FMA obtains information from obliged entities about transactions which bear characteristics matching the FMA-approved and reported typologies, schemes and means in the ML/TF area (para. 5 of Article 4 of the AML/CFT Law).

   According to para. 2 of Presidential Decree 501 of 28 January 2021, the FMA is the legal successor of the rights and obligations of the Financial Monitoring Committee.

b) the FMA, within the limits of its competence, obtains other information prescribed by law, including that concerning various financial transactions above the established threshold such as: prizes, transfers to/from anonymous accounts (deposits), purchase and sale of precious metals or stones and jewellery, transactions of clients registered in offshore zones, cross-border transfers, and others.

   Moreover, if there is reason to believe that a transaction is related to ML/TF, the obliged entity also sends relevant information to the FMA (Article 4 of the AML/CFT Law).

1778. **Criterion 29.3**

a) The FMA may request, obtain and use additional information from obliged entities and state bodies (Articles 10 and 17 of the AML/CFT Law, para. 17 of the Regulations on the FMA approved by Presidential Decree 515 of 20 February 2021).

   For instance, obliged entities are obliged to provide the FMA upon its request with necessary information (documents), including cases when the request is related to the analysis of a suspicious transaction (paras. 13-14 of Presidential Decree 13).

b) The FMA has direct access to, or obtains upon request, financial, administrative and law enforcement information from the information systems and resources of the state bodies of Kazakhstan.

   In particular, the Government of the Republic of Kazakhstan approved the Rules for the State Bodies of Kazakhstan to Provide Information from Their Own Information Systems and Resources upon Request of the FMA (No. 1483 of 23 November 2012) and joint acts among industry-specific agencies (GPO, MoF, MoJ, MIID, ACA, MFA, NSC, MoI). Kazakhstan established a procedure for the FMA to obtain access to databases, in particular, in cooperation with the GPO, the rules and grounds for obtaining information from 36 databases were approved (joint order No. 18/127 of 21 February 2017 of the GPO and MoF).

1779. **Criterion 29.4**

a) the FMA conducts monitoring and tactical analysis of information in order to identify predicate crimes, ML/TF (Article 16 of the AML/CFT Law, subpara. 2 of para. 16 of the Regulations on the FMA approved by Presidential Decree 515 of 20 February 2021).

b) The FMA structure has a Directorate of Strategic Analysis and Risk Assessment whose principal tasks include AML/CFT strategic analysis and organisation of ML/TF risk assessment. The Directorate has functions designed to identify vulnerabilities, risks and threats for the purposes of AML/CFT, to prepare analytical and strategic materials, to collect and process intelligence. Additionally, the Directorate, within the limits of its competence, cooperates with the LEAs in special joint measures and plans (section 2.3 of the Regulations on the Financial Monitoring Department approved by FMA Order No. 89-nk of 6 May 2021).

1780. Criterion 29.5 (Met) – if the FMA has reason to believe that the activities of natural and legal persons are associated with ML/TF, it sends information to the LEAs and special state bodies of the Republic of

Kazakhstan and reports this to the GPO (para. 5-1 of Article 16 of the AML/CFT Law). Once the LEAs and special state bodies authorise a request related to AML/CFT, the information is sent to the requestor (para. 3 of Article 18 of the AML/CFT Law). The above information is transferred through secure communications channels in accordance with joint order No. 89 of 21 June 2021 of the GPO, MoI and FMA and with the Rules of Classifying Information as Restricted Information for Official Use and Engaging with It (Resolution No. 1196 of 31 December 2015 of the Government of the Republic of Kazakhstan).

1781. **Criterion 29.6**

a) the FMA maintains a relevant mechanism for keeping, protecting and ensuring the safe custody of information, data and documents which constitute official, commercial, banking or other legally protected secrets that the FMA obtains in the course of its activities (subpara. 2 of para. 2 of Article 17 of the AML/CFT Law). FMA personnel are obliged to maintain the confidentiality and safe custody of information which constitutes official, commercial, banking or other legally protected secrets that becomes known to them (FMA employee job descriptions)

b) as prescribed by law, FMA personnel obtain permission to engage with information which constitute state secrets. Permission to engage with state secrets implies the assumption of written obligations to comply with the requirements to engage with secret information and liability for failing to do so. (Paragraph 1 of Article 29 of the Law "On State Secrets" and paragraph 2 of Article 20 of the AML/CFT Law).

   Breaches of the requirements to the protection of state secrets and engaging with restricted information for official use entail administrative liability (Article 504 of the CAO). Illegal collection, distribution, disclosure of state bodies and loss of information which constitutes state secrets by carriers entail criminal liability (Articles 185, 186 of the CC).

c) restricted access to devices and information, including computer systems, is granted by FMA internal orders, including as part of the FMA Information Security Policy through specialised information security software (FMA internal orders of 2010, 2011, 2012).

1782. **Criterion 29.7**

a) FMA collects, processes and analyzes information on transactions with money and (or) other property subject to financial monitoring, with subsequent forwarding of analysis results to law enforcement and special state bodies of Kazakhstan (Art. 15-16 of the Law on AML/CFT, par. 13-15 of the Regulation on FMA, approved by Presidential Decree #515 as of 20.02.2021).

   The FMA independently makes a decision on conducting the analysis, sending inquiries, as well as disclosing the results of the analysis to LEAs/foreign partners (para. 1 of the Regulation on the FMA, approved by Presidential Decree #515 of 20.02.2021).The FMA individually makes decisions to conduct analysis, to send requests, and to disclose the analysis results to the LEAs/foreign partners through its Expert Council (FMA Order No. 232-NK of 19 August 2021).

b) the FMA has powers to cooperate with national and foreign competent bodies for the purposes of AML/CFT, including the right to request and obtain necessary information, including in accordance with the principles of reciprocity (Articles 16, 17, 18, 19-2 of the AML/CFT Law).

   There are seven AML/CFT cooperation and interaction agreements with state regulatory bodies and 19 agreements with non-governmental associations.

   There are 39 AML/CFT memoranda of cooperation with foreign FIUs.

c) The FMA is the national financial intelligence unit, which is entrusted with AML/CFT functions (Art. 15-16 of the Law on AML/CFT, paras. 1, 13-15 of the Regulation on the FMA).

d) the FMA is a legal entity whose form of business is a state institution and it is financed from the republican budget of the Republic of Kazakhstan (para. 12 of the Regulations on the FMA approved

by Presidential Decree 515 of 20 February 2021). The FMA budget request is prepared by the relevant department of the FIU and approved by the budget commission of the FIU (Chapter 12 of the Budget Code, FMA Order 9-NK). According to p.2 of Article 31 of the Budget Code, FMA independently uses budgetary funds.

In accordance with paragraph 1 of Article 17 of the Law "On Public Service in the Republic of Kazakhstan", citizens applying for public office must meet the established qualification requirements. The FMA order set qualification requirements to FIU employees and staff selection is done by a contest committee of FIU (№ 269-zh/k dated 08.06.2022). Grounds for termination of public service are provided in paragraph 1 of Article 61 of the Law "On Public Service in the Republic of Kazakhstan".Criterion 29.8 (compliant) the FMA has been a full member of the Egmont Group since July 2011.

Weighting and Conclusion

1783. **R.29 is rated compliant.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

1784. In the 2011 MER, the Republic of Kazakhstan was rated largely compliant with the former R.27. The assessment team noted that there was no statistical information which made it impossible to assess the LEAs' AML/CFT performance.

1785. **Criterion 30.1 –** The Kazakh legislation states that crimes are detected and solved in the course of criminal intelligence and detective activities (CIDA) and pre-trial investigation.

1786. CIDA includes the activities of designated state bodies aimed at detecting, preventing and suppressing crimes, identifying the perpetrators and items and documents relevant to the criminal case.

1787. According to Article 6 of Law 154-XIII, the LEAs engaged in CIDA include internal affairs bodies; national security bodies; anti-corruption authority; economic investigation service.

1788. Even though Law 154-XIII does not allocate the areas of responsibility of the CIDA bodies when it comes to detecting and solving predicate crimes and ML/TF, such powers are practically allocated in accordance with the distribution of competence of these bodies in the relevant regulations that determine the features of their activities.

1789. The CIDA bodies detect, prevent and suppress crimes upon their own initiative or as instructed by the investigator in the criminal case, by engaging in criminal intelligence and detective operations (CIDO).

1790. CIDA materials recording factual data on unlawful acts may be used in criminal proceedings as evidence (Article 120 of the CPC).

1791. Pre-trial investigation means an activity regulated by criminal procedural law performed by the competent bodies with a view to establishing the elements of a criminal offence and detecting the perpetrators, which takes the form of inquiry, preliminary investigation and report.

1792. Pre-trial investigation commences with the registration of an application, a report of a criminal offence with the Uniform Register of Pre-trial Investigation or with the taking of the first urgent investigative action.

1793. ML (Article 218 of the CC) and TF (Article 258 of the CC) offences are classified as crimes that require preliminary investigation.

1794. Article 187 of the CPC establishes the investigative jurisdiction of criminal cases. In ML criminal cases preliminary investigation is conducted by the internal affairs bodies, national security bodies, anti-corruption service or economic investigation service that commenced pre-trial proceedings. Exceptions

include ML crimes classified as corruption-related crimes for they were committed by a special entity[66] who took advantage of his official position (para. 1) of part 3 of Article 218 of the CC), with investigators of the anti-corruption service having exclusive investigative jurisdiction over such cases.

1795. TF cases are investigated by the national security bodies, internal affairs bodies or economic investigation service that commenced pre-trial proceedings.

1796. Criminal procedure law also establishes the investigative jurisdiction of predicate crimes.

1797. Special prosecutors from the prosecution bodies conduct a pre-trial investigation (General Prosecutor Order No. 80 of 18 June 2018 "On Approving the Instruction on Organising Pre-Trial Investigation in the Prosecution Bodies"[67]).

1798. **Criterion 30.2 –** According to Article 180 of the CPC, grounds for the commencement of pre-trial investigation include sufficient data evidencing that there are elements of a criminal offence which include: an application of a natural person or official (head) of a legal person; voluntary surrender; a mass media report; a report of an official of the criminal prosecution body concerning an offence which is being prepared, committed or has been committed.

1799. As per the list of circumstances to be proved in a criminal case set forth in Article 113 of the CPC, it is the responsibility of the criminal prosecution bodies to investigate the financial aspect of criminal activities, including for the purposes established by the FATF Methodology.

1800. If elements of ML and TF are identified during the investigation of a criminal case over a predicate crime, including during a parallel financial investigation, this constitutes grounds for the commencement of ML or TF pre-trial investigation.

1801. Proceeding from the provisions of Article 43 of the CPC, cases over predicate, ML, TF and other crimes, the investigation of which revealed elements of TF, may be consolidated into one case. Given the alternative investigative jurisdiction of ML and TF cases, the pre-trial investigation into such crimes is conducted by the investigation body that commenced the pre-trial investigation into the predicate crime and that identified the elements of ML and TF.

1802. Exceptions include cases in which an investigation into a predicate crime reveals elements of ML committed by a special entity (para. 1) of Part 3 of Article 218 of the CC), the investigation of which is attributed to the exclusive competence of the anti-corruption service, as well as the identification of elements of TF by the anti-corruption service which has no competence to investigate TF criminal cases.

1803. If an ML crime, the investigation of which is attributed to the competence of the anti-corruption service (provided it is committed by a special entity), is detected, the case is to be referred to the anti-corruption service in its entirety (ML and predicate) in accordance with the requirements of Article 187 of the CPC since the fact of the main predicate crime is inextricably linked with its laundering and cannot be investigated in isolation.

1804. By virtue of the provisions of Article 186 of the CPC, the exclusive investigative jurisdiction of a criminal case that another criminal prosecution body considers, constitutes grounds for referring the registered application, report of a crime to the relevant body for further investigation. Besides, if a crime is committed in another location and if it is necessary to take investigative action at the place of its commission, this constitutes grounds for referring the case to another criminal prosecution body.

1805. If during the investigation of a criminal case over a predicate crime, one obtains information about actions that have elements of ML or TF but are not related to the crime under investigation, the materials about the said actions are separated into an independent case (Article 44 of the CPC), and the investigative jurisdiction of the new criminal case is established in accordance with the rules set out in c.30.1.

1806. **Criterion 30.3 –** It is the responsibility of the CIDA bodies (listed in c.30.1) and pre-trial investigative

[66] By a person authorised to perform state functions (public official, deputy) or an equal-status person, official, person occupying an important position.
[67] https://online.zakon.kz/Document/?doc_id=39080958

bodies (officials of the pre-trial investigative body), including the prosecutor, investigator, inquiry body, and inquirer, to identify property that is, or may be, subject to confiscation or constitutes criminal proceeds.

1807. The Kazakh legislation states that the LEAs and special state bodies are empowered to take the following measures (to initiate that these be taken) that ensure that property confiscated and criminal proceeds be recovered: i) freezing transactions involving funds and (or) other property for the purposes of AML/CFT (Article 13 of the AML/CFT Law); ii) temporary restriction on the disposal of property (Article 161 of the CPC); iii) suspending deals and other transactions involving property or withdrawing property for up to 10 days (Article 161 of the CPC); iv) including items recognised as physical evidence into the criminal case files or withdrawing and placing the same for safekeeping, use or sale purposes (Article 221 of the CPC); v) seizing property, including property of equivalent value (Articles 161-163 of the CPC).

1808. See c.4.2 for the procedure for detecting, taking provisional measures and seizing property.

1809. **Criterion 30.4** – The Kazakh legislation states that the special state bodies – the designated foreign intelligence body and the State Security Service of the Republic of Kazakhstan – are not LEAs *per se*[68] but are bodies engaged in CIDA.

1810. Accordingly, during CIDA and pre-trial investigation, the special state authorities are responsible for conducting parallel financial investigations into predicate crimes and have all the responsibilities of the LEAs.

1811. The functions of the customs authorities of the SRC include the detection of violations of customs legislation, while they are not LEAs per se. Under Article 12(6) of the Code of the Republic of Kazakhstan "On Customs Regulation", the customs authorities, within their competence, detect, prevent and suppress criminal and administrative offences following the law. At the same time, they are not empowered to carry out the CIDA, or pre-trial investigation, and in case of revealing signs of a criminal offence, they transfer the relevant materials to the LEAs. The customs authorities also have the right to detain (suspend) cash and/or monetary instruments being transported across the customs border of the Eurasian Economic Union when they receive information provided by the LEAs and/or authorised body on possible involvement in ML or TF, as well as to collect and analyse information on the commission of customs offences, i.e. to conduct a financial investigation. Thus, the obligations of Recommendation 30 apply to customs authorities within the framework of their functions.

1812. **Criterion 30.5 –** According to Law 410-V, preventing, identifying, suppressing, solving and investigating corruption-related crimes fall within the competence of the anti-corruption service.

1813. The anti-corruption service is a LEA, CIDA body, and pre-trial investigative authorities and therefore has all the powers and responsibilities as prescribed by law to detect, trace, initiate the freezing and seizure of assets set out in c.30.3.

Weighting and Conclusion

1814. **Recommendation 30 is rated Compliant.**

Recommendation 31 – Powers of law enforcement and investigative authorities

1815. In the 2011 MER, insofar as the powers of law enforcement and investigative authorities are concerned, the Republic of Kazakhstan was rated largely compliant with the former R.28 as there were certain restrictions in terms of obtaining information at the pre-investigation inspection stage.

1816. In 2014, Kazakhstan enacted a new criminal procedure law (CPC) that abolished the pre-investigation inspection stage.

[68] According to Law 380-IV of 6 January 2011 “On the Law Enforcement Service”, the LEAs include prosecution bodies; internal affairs bodies, state fire service; anti-corruption service and economic investigation service; according to Law 552-IV of 13 February 2021, these include national security bodies, the designated foreign intelligence body and the State Security Service of the Republic of Kazakhstan.
https:// www.adilet.zan.kz

1817. **Criterion 31.1–** The LEAs and special state agencies listed in c.30.1 have the competence to conduct CIDA and pre-trial investigation in criminal cases over predicate crimes, ML and TF. When performing their functions, the competent bodies have a substantial scope of powers to obtain access to all necessary documents and information for criminal prosecution purposes, which include:

a) Obtaining registration data available to Fis, DNFBPs and other natural and legal persons – the CIDA bodies may obtain free of charge and use information relevant to the attainment of CIDA objectives from other institutions (Article 8 of Law 154-XIII). The criminal investigative authorities during a pre-trial investigation may request documents and items relevant to the case from natural, legal persons and officials (Article 122 of the CPC). Documents are forcibly withdrawn during a seizure or search (Articles 252 and 253 of the CPC). The competent bodies may obtain information necessary for them to engage in covert investigative activities and CIDA and attain other objectives they have, taking such information from the SIELSA in accordance with the rules and grounds established by a joint order of the General Prosecutor, Minister of Internal Affairs, Minister of Finance, Minister for Civil Service.

b) Searching persons and premises – powers to conduct the above activities are vested with the CIDA bodies (Article 11 of Law 154-XIII) and the re-trial investigative authorities (Articles 252, 255 of the CPC).

c) Obtaining witness testimony – CIDA may involve interviews of the person (Article 11 of Law 154-XIII). Articles 208-201 and 214 of the CPC regulate the procedure for obtaining witness testimony during the pre-trial investigation. The law makes it possible to organise additional and repeated interviews with the witness (Article 211 of the CPC) and face-to-face questioning (Article 218 of the CPC). If the witness fails to attend without just cause when summoned by the criminal prosecution body, he may be brought in (subjected to compulsory attendance) under Article 157 of the CPC.

d) Collecting and withdrawing physical evidence – in the course of CIDA, it is possible to identify items and documents relevant to the criminal case during such CIDO as interviews, making enquiries, taking samples, controlled purchases, controlled deliveries, surveillance, personal searches of detained persons, seizure of items and documents they have on them, inspections of residential premises and other places, inspections of transport vehicles, and others (Article 11 of Law 154-XIII). Instruments and instrumentalities of crime, subject-matters of crime (objects of unlawful encroachment), money, valuables, and other property obtained as a result of a criminal offence and discovered during an inspection of the incident scene, location or premise, withdrawn during a search, seizure or other investigative actions by the criminal prosecution body – are recognised as physical evidence (Article 118 of the CPC). The legislation establishes a procedure for withdrawing and keeping physical evidence (see c.4.2).

1818. **Criterion 31.2 –**The legislation on CIDA (CIDO) and criminal procedure law (investigative and other procedural actions) establishes methods to detect and investigate predicate crimes, ML and TF.

1819. The CIDA bodies take CIDO overtly or covertly upon their own initiative or in execution of international legal assistance requests. Besides, as instructed by the investigator, the CIDA bodies take covert investigative action. Materials obtained during CIDA may be used in the preparation and taking of investigative action and CIDO and as evidence in criminal proceedings (Article 14 of Law 154-XIII).

1820. The CPC provides for overt and covert investigative actions (these are taken by the CIDA body as instructed by the pre-trial investigation body). The results of covert investigative actions are used as evidence on a par with evidence obtained in the course of overt investigative actions (Article 239 of the CPC).

a) Covert operations – the list of CIDO is set forth in Article 11 of Law 154-XIII and includes: i) general CIDO (16 types in total), including: interview of persons, infiltration, creation of covert enterprises and institutions; imitating criminal behaviour, use of technical means to obtain information; discovery, covert recording and withdrawal of evidence of unlawful acts, their preliminary

investigation, controlled purchase, and others; ii) special CIDO (6 types in total) taken covertly, including: audio and video control of the person or place; intrusion in and (or) inspection of the place and others. A pre-trial investigation may involve such covert investigative actions as audio and video control of the person or place; intrusion in and (or) inspection of the place; surveillance of the person or place; controlled purchase (Articles 231, 242, 247, 248, 250 of the CPC).

b) Communications are intercepted by taking such CIDO and covert investigative actions as searching for information retrieval devices, covert control, interception and retrieval of information transmitted through an electric power (telecommunications) network; covertly obtaining information about connections between subscribers (subscriber devices; covert control of postal and other items (Article 11 of Law 154-XIII, Articles 243, 244,246 of the CPC).

c) The country legislation (Article 11 of Law 154-XIII, Article 245 of the CPC) makes it possible to gain access to computer information by covertly retrieving information from computers, servers and other devices used to collect, process, accumulate and store information. Further, in a pre-trial investigation, the criminal prosecution body may obtain access to computer information also when taking such overt investigative actions as inspection, search, and withdrawal.

d) Controlled delivery may be carried out in the course of CIDA. Such CIDO (covert investigative action) as controlled purchase may also be carried out (Article 11 of Law 154-XIII, Article 250 of the CPC).

1821. **Criterion 31.3 –** The legislation provides for legal mechanisms to identify accounts owned or controlled by natural or legal persons and to ensure that the competent bodies have in place a procedure for identifying assets without giving prior notice to their owner.

a) Information about transactions, accounts, and deposits of their clients (correspondents) constitutes bank secrets. According to Law 2444, information about the presence of bank accounts and bank account numbers of the client, the balance and cash flow in such accounts may be obtained by: i) the state bodies and officials that exercise the functions of the criminal proceeding in respect of criminal cases they consider – based on a written request authorised by the prosecutor; ii) courts in respect of criminal cases they consider based on a relevant procedural decision of the court; iii) the prosecutor in respect of the materials he considers based on a ruling to conduct an inspection (Article 50). Given the above provision of the Law, when it comes to CIDA taken beyond criminal prosecution, the competent bodies are not empowered to obtain information that constitutes bank secrets (with the exception of the opportunity to obtain upon request information available to the FIU that relates to the transaction subject to financial monitoring under Article 18 of the AML/CFT Law). Given that the CIDA is carried out covertly and without notifying the person, this deficiency does not significantly affect the timeliness of the information.

b) The legislation provides for a procedure for the competent authorities to obtain information about the presence of assets (see c.4.2). The Kazakh legislation does not require prior notice to be given to the owner to the effect that the competent authorities are identifying the assets.

1822. **Criterion 31.4 –**Given the provisions of Article 16 of the AML/CFT Law, the FIU's functions include providing – proactively or upon request of the LEAs and special state authorities – information about transactions subject to financial monitoring and cooperating about the information provided.

1823. In light of the above provisions of Article 122 of the CPC, the criminal prosecution bodies may request any information available to the FIU.

1824. According to Article 17 of the AML/CFT Law, the FIU may, acting in cooperation with the state authorities and LEAs/SSAs establish a procedure for exchanging and transferring information, data and documents pertaining to AML/CFT/CPF.

1825. Obtaining information by LEAs/SSAs from the FIU is done under Joint Agreement #1009dsp dated 10/14/2020 by sending written requests authorized by the prosecutor.

Weighting and Conclusion

1826. The competent bodies have a wide range of powers and methods to obtain necessary information during the investigation of predicate crimes, ML and TF.

1827. However, there are restrictions in terms of obtaining information that constitutes bank secrets at the CIDA stage.

1828. **Recommendation 31 is rated Largely Compliant.**

Recommendation 32 – Cash couriers

1829. In the previous MER, Kazakhstan was rated partially compliant with former Special Recommendation IX. The main deficiencies underlying this rating included the following: the customs system as a whole was not used for AML/CFT purposes; the customs authorities were not empowered to seize or restrain currency in case of ML or TF suspicion; no information regarding international cooperation and coordination with immigration or other government authorities was provided.

1830. **Criterion 32.1 –**Kazakhstan is a member of the Eurasian Economic Union. In Kazakhstan, customs-related matters are regulated by the Customs Code of the Eurasian Economic Union (EAEU CRC), while issues not covered by the EAEU legislation are regulated by the Code of Customs Regulation in the Republic of Kazakhstan (RK CRC).[69]

1831. Article 25 of the EAEU CRC established the rules and procedures for the physical transportation of cash and monetary instruments (including bearer negotiable instruments (BNIs)) across the EAEU customs border. For customs regulation purposes, cash and monetary instruments are treated as goods for personal use (EAEU CRC Art.2).

1832. According to Article 2 of the EAEU CRC, the term "monetary instruments" means travelers' cheques, bills of exchange, cheques (bank cheques), and certified securities that certify the obligation of the issuer (the debtor) to pay, but do not indicate the name of a beneficiary, while the term "cash" is defined as money in the physical form of banknotes and coins (except for coins made of precious metals), which are in circulation and represent the legal means of payment in the member states or non-member states (group of states) of the Union, including banknotes and coins that are being or have been withdrawn from circulation and subject to exchange for banknotes and coins in circulation.

1833. These terms are consistent with the definitions of "currency" and "BNIs" in the FATF Glossary.

1834. Kazakhstan has a system of cross-border declaration of goods intended for personal use that are physically transported by natural persons across the EAEU customs border: (i) in accompanied or unaccompanied luggage by natural persons crossing the EAEU customs border; ii) by international mail; iii) by couriers delivering such goods to/ from natural persons who do not cross the EAEU customs border (EAEU CRC Art.256; RK CRC Art.339). The declaration requirements also apply when cash is transported by truck.

1835. In accordance with EAEU CRC Art.257 and RK CRC Art.340, Kazakhstan uses a double channel system which is a simplified customs control system enabling natural persons to independently select either a "green channel" intended for moving goods that are not subject to declaration, or a "red channel" intended for moving goods that are subject to declaration.

1836. The declaration requirements do not apply to cash and monetary instruments transported by natural persons between the Customs Union Member States[70] (Article 25 of the Treaty on the Eurasian Economic Union dated May 29, 2014). Therefore, transportation of currency and BNIs into/from Kazakhstan inside the EAEU is not subject to restrictions and customs declaration, which is not compliant with the

[69] Effective in Kazakhstan since January 1, 2018

[70] At present, the EAEU member states include: the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan, the Kyrgyz Republic and the Russian Federation.

requirements of the Standard.

1837. The declaration requirements apply to goods sent by international mail. Section 147 of the Postal Service Regulation (adopted by Order 14370 of the RK Minister of Information and Communications dated October 27, 2016) prohibits national and foreign cash and monetary instruments from being sent by international mail.[71] Goods sent by international mail shall be presented to the customs authorities for customs control purposes (RK CRC Art.401).

1838. **Criterion 32.2 –**In Kazakhstan, natural persons (except for persons indicated in criterion 32.1) transporting currency cash in an amount exceeding the threshold value are required to file a written declaration.

1839. Pursuant to EAEU CRC Art.260, Par.1, subpar.7, the transported cash and (or) travelers' cheques which total value exceeds USD 10,000 equivalent are subject to customs declaration.

1840. Other BNIs (except for travelers' cheques) are subject to customs declaration irrespective of their nominal value (EAEU CRC Art.260, Par.1, subpar.8).

1841. Cash and monetary instruments are declared by way of completing a passenger customs declaration (PCD). Information that shall be indicated in PCD is determined by Eurasian Economic Commission Board Resolution 124 (as amended on January 12, 2021) and shall include both the value of the declared currency and the identification data of a declarant.

1842. The EAEU CRC (Art.260, Par.17) and the RK CRC (Art.343, Par.17) contain the imperative provisions that require to indicate in the PCD the following information for AML/CFT purposes in respect of cash and monetary instruments transported across the EAEU customs border: (i) details of a document certifying the right of a foreign national or a stateless person to stay in the territory of Kazakhstan and his/her address; (ii) BNI details; (iii) source of cash and BNIs, unless they are owned by a declarant, and information on their intended use; (iv) transportation route and mode, including means of transport.

1843. **Criterion 32.3 –**Kazakhstan uses a threshold declaration system.

1844. **Criterion 32.4 –** With a view to identifying goods transported in breach of the international customs agreements and laws, *inter alia*, by way of non-declaration or false declaration, natural persons may be subject to customs controls (EAEU CRC Art.310, Par.3).

1845. The customs controls include, among other things, requesting explanations (meaningful information for the customs control purposes), examining customs and other documents, *inter alia*, by collecting and reviewing additional information and data, including those requested from the government authorities and other organizations, etc.

1846. Article 13, Par.1, subpar.1 of the RK CRC empowers the customs authorities to request and obtain necessary customs-related information and documents from declarants and inspected persons.

1847. The aforementioned legal provisions also empower the customs authorities to request any information, including information on origin and intended use of currency and BNIs, from natural persons.

1848. Criterion 32.5 – (Partly met). Pursuant to Article 84, Par.3 of the EAEU CRC, declarants are held liable under the legislation of the Member States for non-declaration, false declaration as well as for the provision of invalid documents, including forged documents and/or documents containing knowingly incorrect/false data, to the customs authorities.

1849. According to Article 551, Par.3 of the CAO, non-declaration or false declaration of currency and BNIs that are subject to written declaration transported by natural persons across the EAEU customs border constitutes the administrative offence and is punishable by a fine in the amount of 10 MCI (approximately USD 64 equivalent).[72]

[71] www.adilet.zan.kz

[72] Hereinafter all amounts are calculated at the exchange rate of KZT 478.31 to one US dollar as of July 26, 2022.

1850. Large-scale transportation of non-declared or falsely declared goods (which value exceeds 10,000 MCI (over USD 64,000 equivalent)) across the EAEU customs border constitutes the economic smuggling criminal offence (CC Art.234) which entails criminal liability.

1851. Paragraph 5 of SC Regulatory Resolution No.10 dated July 18, 1997 "On the practical application of legislation imposing criminal liability for smuggling" clarifies that non-declaration or false declaration means submission by a declarant of a customs declaration containing false information about goods (name, value, quantity, etc.) and/or other information required for the custom control purposes or failure to submit a customs declaration containing information about goods to the customs authorities in the process of customs clearance.[73]

1852. The economic smuggling criminal offence is punishable by a fine in the amount of 80 MCI (around USD 512), correctional work or community services for up to 80 hours, or arrest for up to 20 days with or without confiscation of the subject of the criminal offence (CC Art.234, Par.1).

1853. The same action committed repeatedly, or by a person through abuse of his/her office, or with the use of violence against a border or customs officer, or by a group of persons acting in conspiracy, or at exceptionally large scale (i.e. when the value of transported goods exceeds 20,000 MCI or USD 128,000) entails a more severe liability under Article 234, Par 2 of the Criminal Code and is punishable by a fine in the amount of up to 3,000 MCI (up to USD 19,200) or community services for up to 800 hours, or restriction of liberty or imprisonment for up to 3 years with confiscation of property.

1854. The same actions committed by an executive officer through abuse of his/her official powers or by a criminal group constitute a serious criminal offence and are punishable by imprisonment for 3 up to 8 years with confiscation of property under Article 234, Par.3 of the CC.

1855. The criminal law sanctions are not fully proportionate and dissuasive, nor do they apply to persons moving cash and BNIs within the EAEU.

1856. Given that the maximum amount of fines imposed on natural persons under Article 44, Par.2 of the CAO is limited to 200 MCI (around USD 1,280), the sanctions for administrative offence are low, i.e. are neither proportionate nor dissuasive.

1857. **Criterion 32.6 –**Pursuant to Article 18, Par.6 of the AML/CFT Law, the SRC (that discharges, among other things, the customs-related functions) is responsible for collecting information about declared cash and monetary instruments and providing this information to the FIU. However, the collected information is limited, as it does not cover cross-border transportation of currency and BNIs within the EAEU.

1858. The Rules and Procedures of provision by the government authorities of information contained in their own information systems and databases at request of the designated Financial Monitoring Agency (FIU) was adopted by RK Government Resolution 1483 dated November 23, 2012.

1859. The FIU accesses the declaration-related information held by the customs authorities in compliance with the aforementioned Rules and Procedures via the data transmission channel of the single communication system (SCS) of the government authorities operating in the request-response communication mode.

1860. The FIU is also authorized to retrieve information necessary for AML/CT purposes from the SIELSA. According to the Regulation adopted by joint Order No.18/127 issued by the General Prosecutor and Finance Minister on February 2, 2017, the FIU officers may access information kept in the SIELSA, including the Passenger Customs Declarations and Transport Vehicle Declarations databases, on a round-the-clock basis.

1861. The procedure of information exchange between the FIU and the Ministry of Finance is regulated by joint Order 352/68-nk issued by the FMA Chairman and the Finance Minister on April 16, 2021 and April

[73] www.adilet.zan.kz

21, 2021 respectively, that authorizes the FIU officers to access the information system of the SRC.

1862. **Criterion 32.7 –**The principle according to which the customs authorities are required to discharge the assigned functions in coordination with other government authorities is outlined in Art.14, Par.18 of the RK CRC. The RK legislation and joint regulations of the relevant government authorities constitute the legal framework for such coordination and cooperation.

1863. According to the authorities, coordination and cooperation between the customs authorities and the FIU is regulated by Joint Order 351 dated June 4, 2021, that adopted the Procedure of cooperation between the FMA and the SRC in suppressing the shadow economy.

1864. The procedure of AML/CFT coordination and cooperation between the customs authorities and the LEAs and FIU for restraint/ seizure of the currency and/or BNIs transported across the EAEU custom border is established by Finance Minister's Order 193 dated February 15, 2018, that adopted the relevant Regulation.

1865. Coordination and cooperation between the customs and border protection authorities are regulated by Order 504 of the Chairman of the NSC dated November 30, 2013 that adopted the Standard Procedures of crossing the RK state border by natural persons, aircraft, cargoes and goods.

1866. The Regulation on coordination and cooperation between the SRC and the national railway company, the national rail, sea and river carriers, and international air carriers adopted by joint Order 372/195 issued by the Finance Minister and the Investment and Development Minister on March 15, 2018, and March 26, 2018, respectfully established the procedure of coordination between the customs authorities and the carriers in the process of customs clearance of goods and transport vehicles transported across the border.

1867. **Criterion 32.8 –**

c) Pursuant to Article 12, Par.5 and 6 of the RK CRC, the customs authorities are responsible for implementing AML/CFT measures under the international agreement of the EAEU Member States in the process of exercising customs control over transportation of currency and BNIs across the EAEU customs border and also for preventing, detecting and disrupting criminal and administrative offences.

   According to Article 13, Par.1, subpar.14 of the RK CRC, the customs authorities shall seize (restrain) cash and (or) monetary instruments transported across the EAEU customs border upon receipt of information on their potential relation to ML/TF from LEAs and (or) FIU.

   The procedure of seizure (restraint) by the customs authorities of currency and (or) BNIs transported across the EAEU customs border is set out in Finance Minister's Order 193 dated February 15, 2018. The time period of such seizure (restraint) is unlimited.

d) Non-declaration or false declaration in the situations provided for in the legislation entails administrative or criminal liability.

   According to Article 720 of the CAO, administrative proceedings are undertaken by the customs authorities. By virtue of the provisions of Article 795 of the CAO, the customs authorities are empowered to seize currency and BNIs (that are subjects of an administrative offence) as a provisional measure under the administrative proceedings.

   Pre-trial criminal investigations into criminal offences covered by Article 234 of the CC are conducted by the EIS or the ACA (in case of economic smuggling offences committed by executive officers). Transportation of currency and instruments that are subjects of a criminal offence is suspended by a criminal prosecution authority in a manner established in the criminal procedure legislation (see criterion 4.2 for details).

1868. **Criterion 32.9 –**The general period of retention of customs declarations set out in the RK CRC is five years. The legislation regulates the retention of customs declarations when: (b) there is a false declaration; and (c) when there is suspicion of ML/TF.

1869. According to the CAO and the CPC, false declarations serve as evidence for administrative and criminal prosecution and, as such, are included in administrative/ criminal files. A similar procedure is in place for the retention of declarations where ML/TF is suspected. The RK legislation provides for an electronic case management system with the unlimited document retention period

1870. Pursuant to Article 19 Par.6 of the RK CRC, the customs authorities are required to provide backup copies of information held by them to the single electronic data storage system.

1871. In view of the above, the customs authorities are able to provide necessary declaration-related information for the purposes of international cooperation and assistance in situations provided for in the international agreements signed by Kazakhstan.

1872. **Criterion 32.10 –**Pursuant to Article 19, Par.1 of the RK CRC, the customs authorities are required to use information obtained, *inter alia*, through the declaration system only for pursuing the assigned tasks and functions.

1873. Pursuant to Article 19, Par.1 of the RK CRC, the customs authorities are required to provide the collected information to the RK government authorities in situations and in a manner provided for in the legislation and subject to the confidentiality requirements set out in the RK legislation on safeguarding state, commercial, bank, tax and other secrets protected by law and other confidential information and in the international agreements signed by Kazakhstan.

1874. **Criterion 32.11 –**Persons who physically transport currency and BNIs across the border are held administratively and criminally liable if their actions constitute the administrative offences covered by Article 551 of the CAO or the criminal offences covered by Article 234 of the CC which are punishable by sanctions described in criterion 32.5.

1875. If a cross-border transportation of currency and BNIs is related to ML/TF, a natural person may be held criminally liable, *inter alia*, for multiple offences.

1876. Sanctions for ML and TF offences are described in criteria 3.9 and 5.6.

1877. Sanctions for predicate offences depend on the seriousness of such offences. The maximum sanction for medium-grave criminal offences is imprisonment for up to five years, for grave criminal offences – imprisonment for up to 12 years, and for exceptionally grave criminal offences – imprisonment for up to 20 years or life imprisonment.

1878. Article 234 of the CC provides for the confiscation of property as a supplementary sanction. SC Resolution No.10 dated July 18, 1997, provides guidelines regarding the confiscation of smuggled items for the benefit of the state and clarifies that, in case of non-declaration or false declaration, the subject of a smuggling offence includes only currency and BNIs which value exceeds the established threshold, i.e. over USD 10,000, while currency and BNIs which value is below USD 10,000 are not considered the subject of a smuggling offence and shall be returned to their owners.

1879. Article 234 of the CC provides for confiscation of the subject of an administrative offence, which can be used if provided for in the range of the applicable sanctions. Sanctions provided for in Article 551, Par.1 of the CAO do not include confiscation and, therefore, the non-declared or falsely declared currency and BNIs transported by a natural person are not subject to confiscation.

1880. Given the above and in view of the deficiencies identified in criterion 32.5, sanctions are not fully dissuasive and proportionate.

Weighting and Conclusion

1881. Kazakhstan has taken certain steps to implement the R.32 requirements into the national legislation.

1882. n Kazakhstan, the cross-border declaration system applies to cash and BNIs transported across the EAEU customs border; it does not apply to the movement within the EAEU.

1883. Sanctions are not fully dissuasive and proportionate.

1884. **Recommendation 32 is rated Largely Compliant.**

Recommendation 33 – Statistics

1885. In the first round MER, Kazakhstan was rated non-compliant with former Recommendation 32. The identified deficiencies included, in particular, the following: (a) lack of statistical information did not allow for assessing the effectiveness of the work of some LEAs; (b) no steps were taken by the supervisors to review the AML/CFT efforts undertaken by the supervised entities; (c) there was no statistics on the quantity and value of property frozen pursuant to UN Security Council Resolutions; and (d) the effectiveness of the national AML/CFT system was not subject to a regular review.

1886. Criterion 33.1 –

a) Information on transactions that are subject to financial monitoring is documented by obliged entities and submitted electronically to the FMA via the dedicated communication channels (AML/CFT Law Art.10, Par.2; FMA Order 3 of 22.02.2022 Section 2, Par.3).

   In turn, the FMA is responsible for generating and maintaining the national database, which design and functions (approved by the FMC Chairman in 2009) enable to record and store the STRs filed by obliged entities, and also for ensuring methodological consistency and interoperability of the AML/CFT information systems (FMA Statute, Section 16, Par.11).

   For automated collection and recording of STRs received from obliged entities and disseminated to the law enforcement and special government authorities, the relevant subsystems were created within the FMA Single Information System.

b) State legal statistics on investigations, prosecutions and convictions in relation to ML/TF are recorded by the CLSSR of the GPO (Presidential Decree 1050). All necessary information is maintained in the automated “Unified Register of Pre-trial Investigations” (URPI) database. The database contains information on pre-trial investigations (crime registration, qualification of the crime, amount of damage, value of seized property, investigation results, suspects and defendants), prosecutions (conviction or acquittal, review of sentences by higher courts, punishment measures).

   Statistics on ML offenses linked to the predicate offenses, as well as forms (methods) of ML is accumulated by analysis, rather than authomatically. The statistics accumulated in the CLSSR does not contain a separation between the committed crimes of terrorism financing and financing of extremism, due to the fact that both of these crimes are specified in one article 258 of the CC.

c) Ehe statistics do not take into account the differences in the concepts of crime and criminal income, which is not a significant deficiency **.**State legal statistics on confiscated property and criminal proceeds that are subject to recover or recovered by Kazakhstan is maintained by the GPO CLSSR (Law 510-II Art.12, Par.3, subpar.17).

   Compulsory enforcement authorities keep records of executed court decisions in criminal cases regarding the collection of fines, restitution of damages, and confiscation of property, reflecting the amounts recovered.

   Besides that, the designated public property agency coordinates the efforts undertaken for maintaining the consolidated records of public property and the database of property confiscated and appropriated for the benefit of the state (Law 43-IV Art. 24-1). Only the total amount of property received by the state is taken into account. No records are kept of the grounds for confiscation (administrative, civil or criminal proceedings, crimes for which confiscation was applied and the property was returned to the state).

   The CLSSR also uses the URPI to keep records of property sized in the course of pre-trial investigations (as per the statistical form provided in Annex 16 to the Regulation on accepting and registering criminal offence reports and maintaining the single register of pre-trial investigations

adopted by GP Order 89 dated September 19, 2014). The procedure and frequency of compiling statistics on confiscated property seized in course of pre-trial investigations are set out in GP Order 62 dated March 29, 2022.

According to the presented documents, no statistics on frozen funds is maintained by the central government authorities and individual agencies.

d) The state legal statistics on mutual legal assistance and other international requests related to ML/TF is maintained by the Committee on Legal Statistics and Special Records of the RK General Prosecutor's Office (Law 510-II Art.13, Par.3, subpar.18).

Weighting and conclusion

1887. The Republic of Kazakhstan has legally established mechanisms for the collection and processing of various types of statistics. There are minor shortcomings in the collection and accumulation of information on criminal income, the amount of confiscation and frozen funds.

1888. **Recommendation 33 is rated largely compliant.**

Recommendation 34 – Guidance and feedback

1889. In the 2011 MER, Kazakhstan was rated non-compliant for former Recommendation 25, as the supervisory authorities developed no guidelines, including description of ML and TF methods and techniques, for the private sector.

1890. **Criterion 34.1 –** FMA and the supervisory authorities conduct outreach to the supervised entities for providing feedback, clarifying the applicable legislation and identifying suspicious transactions (AML/CFT Law Art.16).

1891. In the personal account on the official website of the FMA the most frequently asked questions and answers are published on a quarterly basis, as well as useful links for use in the work of the FMSA. There are also placed ML/TF typologies, risk indicators, methodological recommendations on criteria and risk indicators of ML (approved by the FMA Chairman on July 2, 2021) and on identification of beneficial owners of legal entities. The manual "Requirements of international standards, typologies and suspicious transactions related to money laundering" was developed, which analyzes examples of specific products and services related to transactions with money and property, which are most vulnerable to ML.

1892. In the section "Distant monitoring" there is an explanation of issues requiring immediate response online (in the message section of the obliged entities and authorities). Approved Requirements for obliged entities to undergo training (October 13, 2020 № 1000 with amendments of August 11, 2021 № 6). Groups were created in messenger chats in which all obliged entities and Associations are included. In these groups information is exchanged daily and around the clock.

1893. A special section on AML/CFT on the official ARDFM website contains explanations and recommendations for obliged entities on identifying beneficial owners and foreign public officials, interaction with residents of jurisdictions with strategic AML/CFT deficiencies or subject to sanctions regimes, on types of fraudulent schemes, including those involving financial pyramids, etc. In addition, the FMSRS informs banks about the typologies and signs of suspiciousness (letters of the ARDFM from 26.11.2018. No. 11-3-16/332/YUL-A-2443, dated 23.01.2019. No. 11-3-11/22/YUL-K-38, No. 06-3-05/1298 of 30.09.2020), as well as on clarification of certain provisions of the AML/CFT legislation.

1894. Certain typologies and guidelines for identifying ML-related offences and the lists of high risk customers (with whom banks refused to establish or terminated business relationships and refuse to carry out transactions on the grounds set out in Article 13, Par.1 of the AML/CFT Law) are posted in the "Risk Factors' module on the National Bank web portal. Exchange offices have been provided with the guidelines clarifying how to complete the AML/CFT compliance reports and inform the employees about changes in the applicable legislation. Training on completion of new forms of regulatory reports was delivered to

obliged entities.

1895. As part of the Action Plan for mitigating risks and improving the effectiveness of AML/CFT efforts, the APDC holds the AML/CFT outreach and awareness raising events for commodity exchanges.

1896. The AFSA has developed the guidance on combating money laundering and applying online CDD measures compiled a consolidated list of ML/TF typology reports and established the requirements for AML training courses delivered by the relevant persons and training centers.

1897. In accordance with the approved plans for conducting explanatory work on compliance with the Laws "On Gambling Business", legislation on AML/CFT in 2019 Ministry of culture and sport held 4 meetings, in 2020 6 meetings, in 2021 5 meetings and in 2022 3 meetings, developed appropriate guidelines, 4 leaflets and sent to obliged entities.

1898. The territorial bodies of justice, in cooperation with the local chambers of notaries and bar associations, carry out legal advocacy work among notaries and lawyers on compliance with the AML/CFT Law. In addition, the Republican Chamber of Notaries and territorial Bar Associations operate training centers for notaries and lawyers. Between 2017 and the first half of 2022 there were 227 seminars and 119 refresher courses on AML/CFT legislation for notaries and lawyers (of which 17,124 notaries and 6,984 lawyers took part).

1899. The FIU concluded about 30 agreements and memorandums in order to cooperate with public associations in the field of AML/CFT.

1900. The rules of sending feedback on the quality of STRs to FIU were approved by the Order of the Chairman of FMA "On approval of rules of sending feedback by Agency of the Republic of Kazakhstan on financial monitoring on the quality of messages about suspicious operations of subjects of financial monitoring". FIU A on an ongoing basis sends letters on deficiencies, quality and opportunities to improve the quality of STRs. The authorities have developed a guidance manual entitled "Requirements of International Standards, Typologies and ML-Related Suspicious Transactions" that examines and analyses specific products and services related to transactions with funds and assets that are most vulnerable to ML.

Weighting and conclusion

1901. Since the previous mutual evaluation, the Republic of Kazakhstan has taken significant steps to address the identified deficiencies on this recommendation. The supervisory authorities have mechanisms for interaction with the FIs on AML/CFT issues, however the guidelines are generally limited to the publication of typology reports and recommendations in terms of ML. Nevertheless, this shortcoming is largely mitigated by the work of the FIU and the functioning of the "Personal Account".

1902. **Recommendation 34 is rated largely compliant.**

Recommendation 35 – Sanctions

1903. Following the first round of the MER, the Republic of Kazakhstan was rated non-compliant with the former R.17. The assessment team noted the following deficiencies: i) there are no sanctions against persons that are not obliged entities; ii) limited sanctions in respect of obliged entities; iii) legal regulatory gaps in the application of sanctions, including supervisors having no relevant powers.

1904. **Criterion 35.1**– Legal persons are not held criminally liable in accordance with the fundamental principles of the Kazakh national legislation.

1905. Natural persons are held criminally liable specifically for ML under Article 218 of the CC and for TF under Article 258 of the CC (see R.3 and R.5 for more detail), as well as administrative liability for committing an ML (Article 214-1 of the CAO) in the form of a fine from 700 MCIs to 2,000 MCIs (from ~$4,650 to the ~$13,200).

1906. Officials of legal entities may be held criminally liable for failing to comply with the AML/CFT/PF

legislation that caused considerable damage or substantially impaired the rights and legitimate interest of citizens or state and public interests, for abuse of office (Articles 250, 251, 361 of the CC), abuse of power (Article 362 of the CC) and other crimes.

1907. Article 214 of the CAO establishes liability of the obliged entities for violations of the AML/CFT legislation. This article provides administrative liability for failure to comply with the regulatory requirements that implement R.6, R.8-R.23.

1908. Administrative fines range from 20 to 500 MCIs (~$130 to ~$3,300) depending on the subject of the offence (natural person, lawyer, notary, official) and the size of the obliged entity (small, medium, large business entity). For repeat commission of administrative offences, Article 214 of the CAO prescribes fine from 100 MCIs to 600 MCIs (~$660 to ~4,000) depending on the subject of the offence and the size of obliged entity.

1909. The penalty amount for a one-time breach of the AML/CFT legislation is insignificant, whereas penalties for systemic breaches of the AML/CFT Law do not reach its maximum value set forth in the general part of the CAO. With that said, the CAO sanctions for this category of offence are not fully proportionate and dissuasive. Available statistics on the number of administrative cases registered under Article 214 of the CAO does not indicate that the sanctions are fully proportionate and dissuasive (see paras. 1015-1025).

1910. The Kazakh legislation establishes sanctions that take the form of license suspension, invalidation or withdrawal. However, this measure may be applied only in respect of certain categories of obliged entities (STBs, insurance companies, securities market participants, PSPs, EEMAs, lawyers) when it comes to AML/CFT breaches.

1911. The ARDFM publishes on its website information about obliged entities that breached legislative requirements, including the AML/CFT ones.

1912. Sanctions similar to those imposed upon VASPs are applied against obliged entities that are AIFC members that failed to comply with the AML/CFT requirements (see c.15.8 (a)).

1913. According to Article 49 of the CIVC, a legal person may be wound up by the court in cases when the former engages in activities in flagrant violation of the law which implies activities prohibited by legislative instruments. These provisions are made more specific, *inter alia*, by restricted interagency instruments which state that there is a regular exchange of information about the incorporation of shell companies and so forth. As part of joint efforts, the court invalidates these organisations.

1914. **Criterion 35.2 –** Officials (directors and senior managers) are perpetrators of economic crimes which fall under Article 218 (Laundering of Funds and (or) Other Property) of the CC and of crimes against the interests of service which fall under Article 250 (Abuse of Office) of the CC, Article 251 (Abuse of Office by Private Notaries, Assessors, Private Pre-Trial Bailiffs, Mediators and Auditors Working in Audit Firms) of the CC, and are deprived of the right to occupy a certain position or to engage in a certain activity for up to five years with a lifelong prohibition to become a senior manager of a financial institution, banking and (or) insurance holding and to be a major member (major shareholder) of a financial institution (para. 2 of part 2 of Article 50 of the CC).

1915. Liability under Article 214 of the CAO applies to natural persons who are obliged entities and to officials (civil servants). Meanwhile, according to the note to Article 30 (Administrative Liability of Officials) of the CAO, civil servants in this Code shall be recognized as persons that carrying out or carried out the functions of a public officer permanently, temporary or on a special power up to the date of commission of administrative infraction or performing or performed organizational management or administrative economic functions in the state institutions, subjects of quasi-public sector, bodies of local self-government up to the date of commission of administrative infraction.

1916. Exceptions are the cases established by Article 214-1 of the CAO (carrying out a transaction with money and (or) other property resulting in the legalisation (laundering) of proceeds of crime). According

to part 1 of the note to Article 214-1 of the CAO, a natural person means a person who permanently, temporarily or under special authority performs organisational and management or administrative and economic functions in a legal person or an employee of such a legal person who is entitled to conduct transactions involving funds and (or) other property in accordance with the Kazakh legislation or the Articles of Association of the legal person, or the BO of such a legal person specified in subpara. 3) of Article 1 of the AML/CFT Law.

1917. Although, by virtue of part 4 of Article 33 of the CAO, if a legal person is held administratively liable, an employee (including an official) of the legal person is released from administrative liability, which impedes the opportunity to impose administrative sanctions upon the directors and senior managers. For instance, part 2 of the note to Article 214-1 of the CAO sets forth that a legal person that voluntarily reports a transaction involving funds and (or) other property that led to money laundering is released from administrative liability if there are no elements of other offences in its actions.

1918. Such disciplinary sanctions as dismissal and disciplinary penalty may be imposed upon personnel of obliged entities who breached the requirements of the AML/CFT legislation (Articles 49, 64 of the Labour Code). Examples cited by the Republic of Kazakhstan indicate that disciplinary sanctions are imposed upon personnel of obliged entities, including heads of divisions, for AML/CFT breaches.

Weighting and Conclusion

1919. The Kazakh legislation provides for criminal, administrative and civil law sanctions for AML/CFT breaches. However, the sanctions enshrined in the CAO are not fully proportionate and dissuasive. Civil law sanctions against a number of obliged entities are not limited to license suspension, invalidation or withdrawal for breaches of the AML/CFT legislation. However, the corrective measures for obliged entities outside AIFC are not sufficiently diverse. There is a restriction in terms of administrative sanctions imposed upon directors and senior managers of obliged entities that are not are not state institutions, entities of the quasi-state sector.

1920. **Recommendation 35 is rated partially compliant.**

Recommendation 36 – International instruments

1921. In the 2011 MER, the Republic of Kazakhstan was rated partially compliant with the requirements applicable to international instruments (the former SR.I and the former R.35). The main deficiencies included: insufficient implementation of the provisions of the Vienna and Palermo Conventions regarding ML criminalisation, BO identification, data keeping and suspicious transaction reporting, and those of the Convention for the Suppression of the Financing of Terrorism that relate to the criminalisation of an act that consists in providing funds to terrorists or terrorist organisations with no intent to engage in terrorist activities or unrelated to a specific act of terrorism. Moreover, there were deficiencies in compliance with the requirements of Article 18 of the Convention for the Suppression of the Financing of Terrorism, there was a lack of legal mechanisms that were necessary under UNSC Resolutions Nos. 1267 and 1373; of procedures for delisting citizens from the lists of persons involved in terrorism and extremism; of mechanisms to grant access to those funds required to satisfy the basic necessities of life under UNSC Resolution 1452.

1922. **Criterion 36.1** – the Republic of Kazakhstan has ratified all necessary conventions required by the FATF Recommendations:

1) The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 20 December 1988, Vienna) was ratified on 29 June 1998;
2) The United Nations Convention against Transnational Organized Crime (Palermo Convention, 13 December 2000, Palermo) was ratified on 4 June 2008;
3) The United Nations Convention Against Corruption (Merida Convention, 31 October 2003) was ratified on 4 May 2008;

4) The International Convention for the Suppression of the Financing of Terrorism (ICSFT, 9 December 1999, New York) was ratified on 2 October 2002.

1923. **Criterion 36.2**– the Republic of Kazakhstan fully complies with the requirements of the ICSFT, Palermo and Vienna Conventions. The deficiencies noted in R.12 regarding national and foreign PEPs and the absence of enhanced ongoing monitoring of relations with PEPs do not make it possible to implement the Merida Convention in full.

Weighting and Conclusion

1924. The Republic of Kazakhstan has implemented most provisions of the Conventions. There nevertheless remain insignificant deficiencies in the full implementation of the Merida Convention.

1925. **R.36 is rated largely compliant.**

Recommendation 37 – Mutual legal assistance

1926. In the 2011 MER, the Republic of Kazakhstan was rated largely compliant with the requirements to mutual legal assistance (the former SR.V and the former R.36). The Report states that deficiencies in ML criminalisation may affect the provision of MLA relating to the freezing, seizure and confiscation of ML-related crimes and of MLA relating to ML investigation and prosecution. Deficiencies in TF criminalisation may affect the provision of MLA in cases of dual criminality. Additionally, legislative instruments do not provide for mechanisms to establish the best venue (jurisdiction) to prosecute the accused.

1927. **Criterion 37.1**– the Kazakh legislation has the necessary legal framework to provide and receive MLA in time, including in cases of ML, TF and predicate crime investigations. The Republic of Kazakhstan may provide MLA both under treaties (Article 557 of the CPC) and in accordance with the principle of reciprocity (Article 558 of the CIVPC).

1928. MLA includes, *inter alia*, delivery of documents (Article 573 of the CIVPC), temporary turnover of a person held in custody (Article 574 of the CIVPC), summons of a person (Article 575 of the CIVPC), procedural action through videoconferencing (Article 575 of the CIVPC), search for, seizure and confiscation of property (Article 577 of the CIVPC), extradition (Chapter 60, Articles 579-595), criminal investigation (Chapter 61, Articles 596-600). The CIVPC also establishes procedures for considering (Article 566) and executing (Article 570) requests, providing information about the execution of requests (Article 567), maintaining confidentiality (Article 568) and refusing to execute requests (Article 569). Moreover, Chapter 62, Articles 601-611, establishes a procedure for recognising and enforcing judgments and rulings of courts of foreign states.

1929. **Criterion 37.2** – Article 559 of the CIVPC establishes central bodies for transferring and executing MLA requests:

- The GPO is an authorised body to take procedural action that requires authorisation from the examining judge (court), to engage in criminal prosecution, to turn over (extradite) persons, to temporarily turn over (extradite) or perform transit transfer, to temporarily transfer persons, to transfer convicts and persons suffering from mental disorders which are subjected to compulsory medical measures, to recognise and enforce judgements, and to consider relevant requests from foreign competent bodies.
- The SC is an authorised body for court proceedings that considers relevant requests from courts of foreign states. The MoI, FMA, ACA, NSC may also provide MLA during procedural action that does not require authorisation from the examining judge (court) and consider relevant requests from foreign competent bodies.

1930. According to part 6 of Article 560 of the CIVPC, the central body may consider a request (instruction, petition) from the requesting party received by email, fax or other communication means. Such a request (instruction) is executed only if its delivery is confirmed or the original request is delivered. The above

provision should be regarded as an advantage since this may considerably reduce request execution time-limits.

1931. The prosecutor's automated workplace has an electronic document management programme called the Kadagalau Uniform Information and Analytical System of the prosecution bodies of the Committee for Legal Statistics and Special Records, taking the form of electronic information records on all types of prosecutorial oversight. The functional capabilities of the Kadagalau system allow the central staff of the GPO and the staff of the prosecution bodies of the regions and those equal to them to perform systemic monitoring of request execution.

1932. The GPO coordinates the efforts of all LEAs in forwarding and executing legal assistance requests in criminal cases, including gathering statistics on such requests. The GPO records all incoming and outgoing requests using report form 7.0 of the automated information system of the Uniform Unified Statistical System, with the report formed through the Kadagalau system.

1933. All instructions are registered in the Kadagalau system where priority to their execution is assigned.

1934. Considering that ML/TF-related requests usually involve requests for the provision of information that constitutes commercial and other legally protected secrets, that relates to restrictions on and seizure of property, which requires authorisation from the court in advance, such requests are forwarded through the GPO in accordance with part 1 of Article 559 of the CIVPC.

1935. The General Prosecutor of the Republic of Kazakhstan issued order No. 112 of 2 October 2017, approving the Instruction on Organising Prosecutorial Oversight over the Application of the Law in International Legal Cooperation which assigns priority to the execution of ML/TF-related requests.

1936. Since July 2019 and considering the amendments into Resolution No. 1453 of 31 December 2004 of the Government of the Republic of Kazakhstan, the competent bodies of the Republic of Kazakhstan have been able to individually forward requests to CIS member states under the Minsk and Chisinau Conventions for procedural action to be taken that does not require authorisation from the court.

1937. **Criterion 37.3** – According to Article 569 of the CIVPC, the requesting party's MLA request (instruction, petition) may be denied as provided for by the treaty of the Republic of Kazakhstan.

1938. If there is no treaty of the Republic of Kazakhstan in place, an MLA request (instruction, petition) should be denied if:

1) if the execution of the request (instruction, petition) contradicts the Kazakh legislation or may undermine the sovereignty, security, public order or other interests of the Republic of Kazakhstan;
2) the requesting party is not reciprocal in this area;
3) the request (instruction, petition) concerns an act that is not a criminal offence in the Republic of Kazakhstan;
4) there is sufficient reason to believe that the request (instruction, petition) is forwarded in order to prosecute, convict or punish a person on the grounds of its origin, social, official or financial position, sex, race, ethnicity, language, religion, beliefs, place of residence or on other grounds.

1939. Although, according to part 1 of Article 558 of the CIVPC, if there is no treaty of the Republic of Kazakhstan in place, legal and other assistance may be provided based on a request from a foreign state or as requested by the central body of the Republic of Kazakhstan in accordance with the principle of reciprocity.

1940. Forwarding such a request to the foreign state, the central body of the Republic of Kazakhstan makes written commitments to the requested party that it will consider the latter's request for similar legal assistance in the future (part 2). In its turn, the central body of the Republic of Kazakhstan considers the foreign state's request only if the requesting party makes written commitments to accept and consider a request from the Republic of Kazakhstan in the future in accordance with the principle of reciprocity (part

3).

1941. If there is no treaty with a foreign state in place, the central body of the Republic of Kazakhstan forwards a legal assistance request to the requested party through diplomatic channels (part 5).

1942. **Criterion 37.4** – the CIVPC does not prevent one from executing MLA requests in cases involving tax crimes or in accordance with the principles of secrecy or confidentiality of Fis/DNFBPs except when the relevant requested information is not subject to transfer in light of circumstances to which professional secrecy or attorney-client privilege applies.

1943. Confidential information and professional secrets are protected, however, there are certain procedures through which such materials become available to the LEAs. Bank secrecy is not an obstruction in this case.

1944. **Criterion 37.5**– According to Article 568 of the CIVPC, as requested by the requesting party, the central body or body authorised to liaise takes additional measures to maintain the confidentiality of receipt of a legal assistance request (instruction, petition), its content and information obtained in the course of its execution.

1945. According to para. 2-1 of Article 19-4 of the AML/CFT Law, the competent bodies maintain the confidentiality of provided information, data and documents and use them only for the purposes stated in the request.

1946. Besides, the country has general confidentiality requirements (para. 1 of Article 47, para. 1 of Article 201, para. 1 of Article 241 of the CIVPC).

1947. Officials working with restricted official information are held liable for breaches of the requirements under para. 6 of Article 504 of the CAO in the form of penalties amounting to 20 monthly calculation indices.

1948. **Criterion 37.6** – According to Article 569 of the CIVPC, a request (instruction, petition) for procedural action that requires authorisation from the examining judge (court) concerns an act that is not a criminal offence in the Republic of Kazakhstan. Accordingly, Kazakhstan will execute MLA requests that do not provide for enforcement measures even in cases when the act specified in the request is not recognised as a criminal offence in Kazakhstan.

1949. **Criterion 37.7** – According to Article 569 of the CIVPC, if there is no treaty in place, a request (instruction, petition) for procedural action that requires authorisation from the examining judge (court) should be denied if the request concerns an act that is not a criminal offence in the Republic of Kazakhstan.

1950. Given the above provision, the Republic of Kazakhstan applies dual criminality provisions when dealing with the execution of MLA requests only when such requests are forwarded in accordance with the principle of reciprocity. If there is a treaty between the Republic of Kazakhstan and the requesting party, the dual criminality rule will apply only if there is a relevant provision to this effect in the treaty.

1951. Denying MLA requests on the grounds that the act is not criminalised concerns only procedural action authorised by the court (judge). To execute such requests, the crime does not necessarily have to belong to the same category or to be similarly termed.

1952. **Criterion 37.8** – According to the CIVPC, the competent bodies have required powers and investigative methods when responding to MLA requests (para. 1 of Article 570, Article 571 of the CIVPC). Certain deficiencies in the implementation of the criteria under R.31 result in insignificant deficiencies in c.37.8.

Weighting and Conclusion

1953. The Kazakh legislation has the necessary legal framework to provide and receive MLA. Certain deficiencies in the implementation of the criteria under R.31 result in insignificant deficiencies in c.37.8.

1954. **R.37 is rated largelly compliant.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

1955. In the 2011 MER, the Republic of Kazakhstan was rated partially compliant with the requirements to MLA relating to freezing and confiscation (the former R.38). The main deficiencies included: there is no legal provision that allows seizing or confiscating property of equivalent value and implementing relevant procedures in relation to proceeds; there is no clear mechanism to coordinate property seizure and confiscation efforts with a foreign state; no consideration was given to the matter of establishing a fund of confiscated property; no consideration was given to the matter of distributing confiscated property among the competent bodies of foreign states that contributed to the confiscation of property; deficiencies in ML criminalisation may come into play when providing MLA in those cases that require ML-related proceeds to be frozen, seized and confiscated.

1956. **Criterion 38.1** – the Republic of Kazakhstan may take prompt action in response to foreign states' requests for the freezing, seizure and confiscation of criminal proceeds to the extent permitted by the national legislation (Articles 163, 559, 577 of the CIVPC, para. 2 of Article 566 of the CIVPC, Article 19-4 of the AML/CFT Law).

1957. **Criterion 38.2**– the Republic of Kazakhstan may exercise powers to provide assistance in cooperation requests that concern confiscation without a guilty verdict (Article 667 of the CIVPC), including in the event of the death of the perpetrator, amnesty, expiry of the statute of limitations for liability to be engaged and so forth in order to identify property acquired by criminal means, funds and other valuables subject to confiscation that serve as redress for the damage done (para. 11 of Article 35 of the CIVPC). However, it is impossible to execute MLA requests relating to confiscation which is not based on conviction in criminal cases in which the accused fled and his place of location is unknown or when the perpetrator is not identified.

1958. **Criterion 38.3** – the Republic of Kazakhstan has acceded to most international instruments in the MLA area relating to seizure and confiscation, including the Vienna, Merida, Palermo and Chisinau Conventions. Furthermore, Kazakhstan has entered into a number of bilateral MLA agreements that provide for coordination and cooperation mechanisms in searching for, seizing and confiscating assets. As submitted by the evaluated country, some provisions that pertain to the management of property under the Chisinau Convention apply directly.

1959. Mechanisms for seizing, recording, keeping, transferring, using (including through discarding) confiscated property are regulated by Resolution No. 1291 of 9 December 2014 and Resolution No. 833 of 26 July 2020 of the Government of the Republic of Kazakhstan. Certain deficiencies in the implementation of c.4.4 result in insignificant deficiencies in c.38.3.

1960. **Criterion 38.4**– According to para. 6 of Article 577 of the CIVPC, as petitioned by the central body of the Republic of Kazakhstan, the court may decide to transfer confiscated property or its monetary equivalent:

1) to the requesting party that resolved to confiscate property as redress for the damage done by the criminal offence;

2) in accordance with the treaties of the Republic of Kazakhstan that address the matter of distribution of confiscated property or its monetary equivalent.

1961. The competent bodies may deduct expenses incurred in the course of search, seizure, confiscation and return of funds and (or) other property.

1962. According to Article 19-4 of the AML/CFT Law, the competent body and MoJ may enter into treaties in accordance with the legislation and in each separate case agree on the distribution of funds and (or) property acquired during confiscation or of money after confiscated property was sold.

Weighting and Conclusion

1963. The Republic of Kazakhstan may provide MLA associated with identification, freezing, seizure and

confiscation. However, there are insignificant deficiencies in the management of virtual and complicated assets.

1964. **R.38 is rated largely compliant.**

Recommendation 39 – Extradition

1965. In the 2011 MER, the Republic of Kazakhstan was rated partially compliant with the requirements to extradition (the former R.39). The main deficiencies included: dual criminality is necessary for extradition, and in this respect deficiencies in ML and TF criminalisation may affect the execution of requests; legislative instruments do not provide for mechanisms to establish the best venue (jurisdiction) to prosecute the accused.

1966. **Criterion 39.1**– According to Article 529 of the CIVPC, the General Prosecutor or designated prosecutor may apply to the competent body of a foreign state with a request for the extradition of a Kazakh national who committed a crime if a guilty verdict or indictment order is issued in relation to the person.

1967. According to Article 531 of the CIVPC, the General Prosecutor of the Republic of Kazakhstan or designated prosecutor also consider requests for the extradition of foreign nationals accused of crimes committed or prosecuted in the territory of the foreign state, with the instructions of the above persons constituting grounds for extradition. If the extradition requests conflict with each other in terms of what state the person should be extradited to, the General Prosecutor of the Republic of Kazakhstan makes the relevant decision.

1968. The national legislation regulates the extradition of persons, including those involved in ML/TF (Chapter 60 of the CIVPC; para. 3 of Article 557, para. 1 of Article 558, Articles 588, 589, 591, 590 of the CIVPC; the Convention "On Legal Assistance and Legal Relations in Civil, Family and Criminal Cases" of 22 January 1993 and of 7 October 2002; legal assistance and extradition treaties (entered into with 20 states). The principle of reciprocity in legal assistance matters applies in relation to states with which there is no treaty basis.

a) According to the Kazakh legislation, ML- and TF-related crimes constitute grounds for extradition (para. 1 of Article 579, Articles 218 and 258 of the CC).

b) The Republic of Kazakhstan regulates a special electronic recording procedure for extradition requests and ensures that it assign priority to ML/TF-related requests (subparas. 2 and 3 of para. 12 of the Instruction on Organising Prosecutorial Oversight over the Application of the Law in International Legal Cooperation approved by Order No. 112 of 2 October 2017 of the General Prosecutor of the Republic of Kazakhstan).

c) Article 590 establishes procedures for denying extradition which are not unreasonable or excessively restrictive conditions (reasonable legislative provisions for extradition denial in the evaluated state).

1969. **Criterion 39.2**– A Kazakh national is allowed to be extradited when this is provided for by the treaty (para. 1 of Article 590 of the CIVPC) and is not contrary to Article 11 of the Constitution of the Republic of Kazakhstan.

a) The Kazakh legislation establishes a procedure for taking over criminal proceedings from foreign states and grounds for the denial of further criminal prosecution (Chapter 61 of the CIVPC). The relevant provision is included in all bilateral treaties that concern extradition to which the Republic of Kazakhstan is a party.

b) The existing bilateral treaties enshrine that, if the requested party does not extradite its national, it should prosecute this person under its national legislation.

1970. **Criterion 39.3** – As grounds for extradition denial, the CIVPC establishes a number of requirements that correlate with international legal standards (Article 590 of the CIVPC), and differences in the qualifying factors of crimes do not constitute grounds for extradition denial.

1971. **Criterion 39.4** – The national legislation does not provide for simplified extradition. Only certain treaties provide for a simplified extradition mechanism, including treaties with Brazil (Article 17); Hungary (Article 10); Macedonia (Article 10); Ukraine (Article 11); Italy (Article 16). However, Article 581 of the CIVPC provides for temporary extradition and states that if delays in the extradition of a person may lead to the expiry of the statute of limitations for criminal liability to be engaged or to the loss of evidence in a criminal case, a temporary extradition request may be forwarded.

Weighting and Conclusion

1972. In the evaluated state, ML and TF may constitute grounds for the extradition of a person to another country provided that reasonable conditions are met and his rights are protected. The grounds listed in the CIVPC make it possible to conclude that the grounds for denying extradition enshrined in the legislation of the evaluated state are reasonable. Kazakhstan allows for the extradition of its nationals upon request of a foreign state in certain cases. The county also has certain simplified extradition mechanisms.

1973. **R. 39 is rated largely compliant.**

Recommendation 40 – Other forms of international cooperation

1974. In the 2011 MER, Kazakhstan was rated largely compliant with the requirements related to other forms of international cooperation (former Recommendation 40). The identified deficiencies included the following: there was low level of international cooperation with foreign supervisors; the FIU powers in regard to information exchange in the absence of the relevant international agreements were not clearly defined; and provision of information requested by foreign counterparts could be subject to unduly restrictive conditions.

General principles

1975. **Criterion 40.1**– Kazakhstan ensures that all competent authorities can provide a wide range of international cooperation in relation to ML, TF and predicate offences. The competent authorities can cooperate with foreign counterparts under the international agreements or on the basis of reciprocity (AML/CFT Law Art.3-1).

1976. **Criterion 40.2**

a) The competent authorities have the lawful basis for providing cooperation (AML/CFT Law Art.3-1);

b) The RK competent authorities are authorized to cooperate directly with foreign government authorities and international and regional organizations. The applicable regulations allow them to use secure international, regional and other protected communication channels.

c) The competent authorities can use both open (postal mail, e-mail) and secure (couriers and dedicated secure channels) communication channels to share information with foreign competent authorities.

   With a view to cooperating with foreign competent authorities, different international information exchange networks are used:

   - Egmont Group (an information exchange network comprising nearly 170 FIUs across the globe);
   - CARIN – Europe;
   - ARIN AP – Asia;
   - Interpol I-24/7 information and communication system;
   - OSINT or open sources.

1977. Requests are forwarder by the RK central authority to foreign countries by mail and, in case of emergency, by e-mail, fax or other means of communication. In the latter case, the original request is mailed within three days following its transmission by e-mail, fax or other means of communication (CPC Art.560,

Par.4).

d) The designated authority may, but is not obliged to prioritize execution of requests of foreign competent authorities under Article 19-2, Par.5 of the AML/CFT Law.

e) Unauthorized disclosure of pre-trial investigation information is prohibited by law (CPC Art.201, Par.1, Art.241, Par.1; CC Art. 223 and 423; CAO Art.504; AML/CFT Law Art.18, Par.2, subpar.4, Art.19-2, Par.4-5, Art.20, Par.2).

1978. Criterion 40.3 (met) – The competent authorities are authorized to enter into international agreements needed for discharging their functions and establish direct contacts on the basis of reciprocity (Law on International Agreements of the Republic of Kazakhstan Art.2, Par.3; AML/CFT Law Art.19-1, Par.7 and Art.19-4, Par.14).

1979. Criterion 40.4 (Met) – Provision of feedback to foreign competent authorities is regulated by conventions acceded by Kazakhstan and international agreements signed by Kazakhstan, including international interagency agreements. Feedback is provided using the same procedures that apply to exchange of AML/CFT information (Chisinau Convention Art.74; Egmont Principles of Information Exchange Section 19).

1980. **Criterion 40.5**

a) Although the Criminal Procedure Code does not prohibit competent authorities from executing requests on the grounds that a request involves fiscal matters and confidential information, the legislation (CPC Art.569, Par.2, subpar.1) allows for the possibility of refusing a request by merely referring to the fact that such request is considered to be contrary to the interests of Kazakhstan.

b) Although the Criminal Procedure Code does not prohibit competent authorities from executing requests on the grounds that the laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies) and/or that a request involves fiscal matters and confidential information, the legislation (CPC Art.569, Par.2, subpar.1) allows for the possibility of refusing a request by merely referring to the fact that such request is considered to be contrary to the interests of Kazakhstan.

c) Although the Criminal Procedure Code does not prohibit competent authorities from executing requests on the grounds that there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding, the legislation (CPC Art.569, Par.2, subpar.1) allows for the possibility of refusing a request by merely referring to the fact that such request is considered to be contrary to the interests of Kazakhstan.

d) Although the Criminal Procedure Code does not prohibit competent authorities from executing requests on the grounds that the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart, the legislation (CPC Art.569, Par.2, subpar.1) allows for the possibility of refusing a request by merely referring to the fact that such request is considered to be contrary to the interests of Kazakhstan without clarifying what such contradiction exactly means.

1981. **Criterion 40.6** – The legislation provides for controls and safeguards to ensure that the exchanged information is used in a confidential manner (CPC Art.47, Par.1, Art.201, Par.1, Art.568; AML/CFT Law Art.19-2, Par. 4-5, Art.19-3, Par.3; Art.13 of the AML/CFT Agreement of the CIS Member Countries dated October 5, 2007).

1982. **Criterion 40.7** – The legislation provides for controls and safeguards to ensure that the exchanged information is used in a confidential manner (CPC Art. 568; AML/CFT Law Art.19-2, Par.4-5 and Art.20, Par.2; Principle of Information Exchange between FUIs, AML/CFT MoUs signed by the FIU with foreign counterparts).

1983. **Criterion 40.**8 – The legislation permits to conduct inquiries on behalf of foreign counterparts in the course of providing legal assistance under CPC Art.570, Par.1-2 and Art.56.

Exchange of information between FIUs

1984. **Criterion 40.9** – The FMA is authorized to provide international cooperation to foreign competent authorities, irrespective of their status (whether administrative, law enforcement, judicial etc.), for identifying natural persons, entities and beneficial owners linked to ML/TF, other associated offences and transactions with funds and (or) other assets and for tracing funds and (or) other assets owned by such persons (AML/CFT Law Art.19-2; Section 17, Par.1 of the FMA Statute adopted by Presidential Decree 515 dated February 20, 2021).

1985. The FMA cooperates with the relevant foreign authorities on AML/CFT matters on the basis of reciprocity by way of requesting and sharing information (AML/CFT Law Art.19-1, Par.2).

1986. **Criterion 40.10** – The FMA, being the Egmont Group member, provides feedback as required by Section 19 of the Egmont Principles of Information Exchange. The FMA executive officer is required to provide feedback to foreign competent authorizes on the use of information received at request (Section 21 of the Regulation on AML/CFT cooperation and information exchange with foreign competent authorities adopted by FMA Order 255-NK dated August 8, 2022).

1987. **Criterion 40.11**

a) The FA is empowered to exchange AML/CFT related information with foreign competent authorities both spontaneously and at request (AML/CFT Law, Art.17).

b) The AML/CFT Law (Art.17 and 19-2) does not establish conditions that would make the exchange of information by the FMA with foreign counterparts contingent upon the method or the mode (i.e. direct or indirect) of acquiring information.

Exchange of information between financial supervisors

1988. **Criterion 40.12** – According to Article 19-3 of the AML/CFT Law, the government authorities responsible for monitoring compliance of obliged entities with the AML/CFT legislation within their purview cooperate with the relevant foreign counterparts, *inter alia*, by way of sharing experiences and information related to regulation, monitoring and supervision of obliged entities.

1989. **Criterion 40.13**– The financial supervisors have the powers (see analysis of R.26 and R.27) to exchange internationally the AML/CFT related information available to them domestically (AML/CFT Law Art.19-3).

1990. **Criterion 40.14**

a)-c) Article 19-3, Par.2 of the AML/CFT Law empowers the supervisors to exchange with foreign counterparts information on:

- Implementation of the RK legislation requirements;
- Obliged entities (their activities, business reputation, management structure, beneficial owners);
- AML/CFT internal control programs, policies and procedures of obliged entities;
- Laws and regulations in force in Kazakhstan;
- Outcomes of due diligence conducted on customers, bank and other accounts, business relationships and transactions.

1991. Thus, the supervisors are able to exchange information and/or documents that may be required by foreign counterparts for supervision, which means that the scope of information that can be exchanged is broad enough and includes regulatory, prudential and AML/CFT information. However, the deficiencies identified in R.10 and R.22 may limit the scope and accuracy of exchanged information.

1992. **Criterion 40.15** – The financial supervisors are able to provide assistance to foreign supervisory authorities and take part in monitoring by foreign supervisors of their supervised entities operating in Kazakhstan (AML/CFT Law Art.19-3, Par.1, subpar.3). However, the legislation does not provide for a possibility to authorize or facilitate the ability of foreign counterparts to conduct inquiries and investigations themselves in Kazakhstan in order to facilitate effective group supervision.

1993. **Criterion 40.16** – The financial supervisors are not permitted to disclose the exchanged information to third parties or use the information and documents in breach of the terms and conditions set by foreign competent authorities that provided such information and documents at request (AML/CFT Law, Art.19-3, Par.3, subpar.2)

Exchange of information between law enforcement authorities

1994. **Criterion 40.17** – The law enforcement authorities are able to exchange domestically information, including at the criminal intelligence gathering and preliminary investigation stages, that is available to them domestically (AML/CFT Law Art.19-4, Par.1-3).

1995. **Criterion 40.18** – The legislation permits the competent authorities to use their powers for gathering information necessary for conducting investigations on behalf of foreign counterparts and executing foreign cooperation requests (CPC Art.557,Par.1-2 and Art.558). Operation of the Interpol National Central Bureau in Kazakhstan is regulated by the joint Order on coordination of international search and execution by competent authorities of incoming and outgoing Interpol requests and their processing by the Interpol National Central Bureau in Kazakhstan (joint Order 481 of General Prosecutor's Office, Ministry of Finance, Ministry of Defense, Ministry of Foreign Affairs, Ministry of Internal Affairs, Anti-Corruption Agency, Financial Monitoring Agency, State Security Service, National Security Committee and Supreme Court). Kazakhstan is a member of Camden Asset Recovery Interagency Network (CARIN) since 2017, with the General Prosecutor's Office designated as the focal point. Kazakhstan is also a member of Asset Recovery Interagency Network – Asia Pacific (ARIN-AP) since 2017, with the General Prosecutor's Office, the Ministry of Internal Affairs and the Financial Monitoring Agency designated as the focal points.

1996. **Criterion 40.19** – The legislation contains provisions that authorize the law enforcement authorities to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations (CPC Art.572 and 578; Agreement on creation and operation of joint investigation teams in the territory of the CIS member countries dated October 16, 2015; Article 63 of Chisinau Convention).

Exchange of information between non-counterparts

1997. **Criterion 40.20** – Article 19-2, Par.3of the AML/CFT Law permits the designated government agency to request from foreign competent authorities information and documents on behalf of the domestic law enforcement and special authorities.

1998. As for the incoming international requests, the legislation does not explicitly permit, but also does not prohibit indirect exchange of information by other competent authorities.

Weighting and conclusion

1999. All competent authorities have the powers and ability to provide a wide range of international cooperation. However, there are minor deficiencies related to cooperation by financial supervisors and restrictions that impede information exchange.

2000. **Recommendation 40 is rated largely complaint.**

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 main deficiencies are associated with the need to refine approaches to the identification and assessment of TF and PF risks, as well as in the obliged entities sectors, develop mechanisms for disseminating the risk assessment report information to SRBs, FIs and DNFBPs, build a comprehensive risk-based approach to implementing risk mitigation measures, as well as synchronize the exemptions from customer identification obligations with the findings of specific national or sectoral risk assessments.
2. National cooperation and coordination	C	
3. Money laundering offence	LC	• The sanctions against legal persons for ML classified as an administrative delict are not fully proportionate and dissuasive.
4. Confiscation and provisional measures	LC	• The procedure for the evaluation of property subject to confiscation at the pre-trial stage is not regulated in detail by the legislation. • Freezing (suspension of transactions with funds or other assets) is not applicable to criminal cases of predicate offences (except TF). • The legislation contains no provisions regarding the mechanisms of the management of VA, as well as complex assets.
5. Terrorist financing offence	LC	• Does not criminalize the financing of terrorist organizations that have not been recognized as such by a court or that are not designated in the UN sanction lists. • The liability of legal persons is limited to their liquidation through civil proceedings, such sanction is not proportionate in all cases.
6. Targeted financial sanctions related to terrorism and terrorist financing	PC	• The legislation does not contain legally binding requirements covering all natural and legal persons (not only FIs and DNFBPs), which relate to the freezing of funds or other assets, as well as the prohibition to provide funds/assets/services to natural or legal persons designated in the sanction lists.
7. Targeted financial sanctions related to proliferation	PC	• The legislation does not contain legally binding provisions that apply to all natural and legal persons (and not FIs and DNFBPs) that require them to freeze funds or other assets and prohibit them from making funds/ assets/ services available to natural or legal persons included in the sanction lists.

8. Non-profit organizations (NPOs)	LC	• In practice, the MISD applies a risk-based approach to AML/CFT supervision, but the mechanism for its response, as well as that of other concerned government authorities, to the identified threats is not fully defined in the regulations.
9. Financial institution secrecy laws	LC	• - The restrictions on access to bank secrecy information in the execution of international requests; • No provisions in legal acts allowing FIs, except for STBs, to exchange information constituting banking, commercial or other legally protected secrets with other FIs.
10. Customer due diligence (CDD)	LC	• Some low-risk occasional transactions are excluded from the requirement to implement CDD measures in case of a suspicious transaction. • Some deficiencies concern possibility for FIs not to pursue the CDD process and instead file an STR. •
11. Record keeping	LC	• There are restrictions on direct access to information for public authorities other than the FIU and supervisory bodies
12. Politically exposed persons	LC	• Additional measures do not apply to foreign PEPs and PEPs of international organisations who have ceased to perform their functions, nor do they include ongoing enhanced monitoring of the business relationship • No specific requirement for measures to determine whether the PEP is the beneficiary or the beneficial owner of the beneficiary
13. Correspondent banking	LC	• No requirements for other similar relationships
14. Money or value transfer services (MVTS)	LC	• Payment agents and payment sub-agents of payment systems are not subject to licensing or registration requirements; • The KazPOst is exempt from these requirements as it is permitted to carry out certain types of banking transactions without a license.
15. New technologies	PC	• There are no requirements for exchange offices to identify or assess ML/TF risks for new products or to assess risks before launching new products, business practice or use of new or emerging technologies, that corresponds. • The AFSA assessed the ML/TF risks of virtual assets and VASPs sector as part of the NRA, however, vulnerability and risk analysis specific to AIFC members and not the VASPs generally in the country. • Measures to mitigate the risks identified for VASPs outside AIFC are insufficient.

		• VASP outside AIFC, that is a natural person, is not required to be registered or to obtain a license. • There are no requirements to check BOs and affiliates of VASPs outside AIFC for criminal records; • The interaction is less about feedback for VASPs • No possibility to impose administrative sanctions on officials of VASPs outside AIFC if they are not quasipublic entities. • There are deficiencies in terms of compliance with requirements of R. 16 for VASP outside AIFC.
16. Wire transfers	LC	• Requirements for information to accompany wire transfers do not apply to money transfers between natural persons using payment cards • Exclusion of payments and money transfers using payment cards is not subject to the requirement that the payment card number be indicated for all transfers in a transaction.
17. Reliance on third parties	LC	• No condition that any heightened country risk is fully offset by the AML/CFT mechanisms of the financial group, in case the obliged entity participating in the group relies on CDD measures taken by other participants in such group; • AIFC participants may rely on third parties to carry out ongoing monitoring of the business relationship, that contradicts R.17.
18. Internal controls, foreign branches and subsidiaries	LC	• There are shortcomings regarding the exchange of information and the application of compliance, audit and AML/CFT functions at group level.
19. Higher risk countries	LC	• Minor weaknesses related to the lack of requirements on the proportionality of CDD measures to risks
20. Reporting of suspicious transactions	C	
21. Tipping-off and confidentiality	C	
22. DNFBPS: customer due diligence	LC	• Deficiencies under R.10 and R.12 are applicable to DNFBPs • no regulations ensuring that any information obtained at CDD matches relevant details of a specific client transaction • No obligation for real estate agents to apply CDD measures to both the buyer and the seller; •
23. DNFBPS: other measures	LC	• Some shortfalls are highlighted in connection with compliance with the requirements of R.19.
24. Transparency and beneficial ownership of legal persons	PC	• The legal entity risk assessment carried out is not complete and comprehensive; • Data on BO in SDLP is not verified;

		• No provisions for regular updates of information in the register and commensurate liability for failure to meet most of the recommendation criteria; • No disclosure requirements for nominee shareholders and directors; • No regulations on monitoring the quality of assistance from other countries in response to requests for basic and beneficial ownership information, or the tracing of the BO abroad.
25. Transparency and beneficial ownership of legal arrangements	LC	• No statutory requirements for the operation of trusts and other legal arrangements, except in the AIFC area; • AIFC has transparency requirements for BOs of trusts, while at the same time there is vague and assessable language on disclosure obligations; • No legal provisions for proportionate and dissuasive sanctions (criminal, civil or administrative) for failure to provide competent authorities with timely access to trust information, except for the AIFC.
26. Regulation and supervision of financial institutions	PC	• the legislation does not provide for all measures to prevent criminals or their associates from holding significant shares or having access to management functions in FIs. No requirement to take into account the ML/TF risks existing in the country when applying the RBA in supervision; • No legal act on how to conduct consolidated AML/CFT supervision in relation to financial groups.
27. Powers of supervisors	LC	• The lack of authority of the NB to exclude PSPs from the register. • The lack of authority of the APDC to impose disciplinary sanctions on commodity exchanges for non-compliance with AML/CFT requirements. • Most supervisory authorities do not have the authority to impose financial sanctions themselves.
28. Regulation and supervision of DNFBPS	PC	• Persons associated with the BOs of DNFBPs are not identified; • Not all DNFBP officials can be held administratively liable; • Types of corrective actions are not sufficiently diverse or dissuasive. • Risk-based supervision of the DNFBPs does not take into account the type and number of DNFBPs and the ML/TF risk profile.
29. Financial intelligence units	C	•
30. Responsibilities of law enforcement and investigative authorities	C	

31. Powers of law enforcement and investigative authorities	LC	• There are restrictions in terms of obtaining information that constitutes bank secrets at the CIDA stage.
32. Cash couriers	LC	• In Kazakhstan, the cross-border declaration system applies to cash and BNIs transported across the EAEU customs border; it does not apply to the movement within the EAEU. • Sanctions are not fully dissuasive and proportionate.
33. Statistics	LC	• Statistics on ML/TF investigations, prosecutions, and convictions are not fully comprehensive. Statistics on ML offenses linked to predicate offenses, as well as forms (methods) of ML are not maintained. The statistics accumulated in the CLSSR does not distinguish between the committed crimes of terrorism financing and financing of extremism, since both of these crimes are mentioned in the same Article 258 of the CC. • No records are kept of the proceeds of crime. No statistics are kept on the types of property seized (criminal proceeds, instrumentalities and means of crime, property intended for TF, property of corresponding value). • Compulsory enforcement authorities keep records of executed court decisions in criminal cases regarding the collection of fines, restitution of damages, and confiscation of property, showing the amounts recovered. Statistical records of confiscation by crimes are not kept. • Only the total amount of property received by the State is recorded in the statistics. No records are kept on the grounds of confiscation (administrative, civil or criminal proceedings, offences for which confiscation was applied and the property was returned to the State)
34. Guidance and Feedback	LC	• The guidelines, in general, are limited to the publication of typology reports and recommendations in terms of ML. Nevertheless, this shortcoming is largely offset by the work of the FIU FMA and the functioning of the "Personal Account".
35. Sanctions	PC	• The sanctions imposed by the CAO are not fully proportionate and dissuasive; • Corrective measures in relation to obliged entities in Kazakhstan are not sufficiently diverse; • There is a restriction on the application of administrative liability measures to directors and senior management of those obliged entities that are not quasipublic entities.
36. International Instruments	LC	• The procedure for prioritizing requests is not clear enough;

		• Non-coercive MLA requests will be executed by Kazakhstan, even if the act for which the request is made is not recognized as a criminal offence in Kazakhstan.
37. Mutual Legal Assistance	LC	• Certain deficiencies in the implementation of the criteria under R.31 result in insignificant deficiencies in c.37.8.
38. Mutual Legal Assistance: Freezing and Confiscation	LC	• There are insignificant deficiencies in the management of virtual and complicated assets.
39. Extradition	LC	• There are minor deficiencies, particularly with regard to cooperation by financial supervisors, as well as established restrictions that impede information exchange. •
40. Other Forms of International Cooperation	LC	• The procedure for prioritizing requests is not clear enough; • Non-coercive MLA requests will be executed by Kazakhstan, even if the act for which the request is made is not recognized as a criminal offence in Kazakhstan.

GLOSSARY OF ACRONYMS

AI	Authorized institutions (performing foreign currency exchange transactions in cash)
AIFC	Astana International Financial Center
AML/CFT/CPF	Anti-money laundering, countering the financing of terrorism and countering proliferation financing
BO	Beneficial owner
CDD	Customer due diligence
CIDA	Criminal Intelligence and Detective Activity or Operational-Investigative Activity
CIDO	Criminal Intelligence and Detective Operations or Operational-Investigative Means
CIS	Commonwealth of Independent States
DNFBP	Designated non-financial businesses and professions
EAEU	Eurasian Economic Union
EECTBO	Entities engaged in certain types of banking operations
EEMA	Entities engaged in microfinance activities
FI	Financial institution
ICR	Internal control rules
Jewelers	Individual and corporate dealers in precious metals, precious stones and jewelry
KazPost	“KazPost” JSC, the national postal operator in the Republic of Kazakhstan
LEA/SSA	Law enforcement authorities and Special state agencies
MCI	Monthly calculation indicator (an indicator used in Kazakhstan to calculate pensions, benefits and other social payments, as well as to apply penalties, calculate taxes and other payments, as well as in agreements on joint activities)
ML NRA	National money laundering risk assessment
NPO	Non-profit organization

Obliged entity	Obliged entity that is subject to financial monitoring
Organisers of gambling industry	Casinos, gaming machine halls, bookmaker offices, totalizators, lottery
PSP	Payment servise providers
URPI	Unified Registry of Pre-trial Investigations
Competent authorities	
FMA	Financial Monitoring Agency of the Republic of Kazakhstan
FMD	Financial Monitoring Department of the Financial Monitoring Agency of the Republic of Kazakhstan
ARDFM	Agency for Regulation and Development of Financial Market of the Republic of Kazakhstan
AFSA	Astana International Financial Center Financial Services Authority
APDC	Agency for Protection and Promotion of Competition of the Republic of Kazakhstan
CLSSR	The Committee on Legal Statistics and Special Records under the Prosecutor's General Office
EIS, EID	Economic Investigation Service of the Financial Monitoring Agency of the Republic of Kazakhstan, Department of economic investigations
NB	National Bank of Kazakhstan
MIID	Ministry of Industry and Infrastructure Development of the Republic of Kazakhstan
MISD	Ministry of Information and Social Development of the Republic of Kazakhstan
MCS	Ministry of Culture and Sports of the Republic of Kazakhstan
MoF, SRC	Ministry of Finance of the Republic of Kazakhstan, State Revenue Committee of the Ministry of Finance
MDD	Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan
MoJ	Ministry of Justice of the Republic of Kazakhstan
ME	Ministry of Economy of the Republic of Kazakhstan

ACA	Anti-Corruption Agency of the Republic of Kazakhstan
SC	Supreme Court of the Republic of Kazakhstan
GPO	General Prosecutor's Office of the Republic of Kazakhstan
MIA	Ministry of Internal Affairs (Interior Ministry) of the Republic of Kazakhstan
NSC	National Security Committee of the Republic of Kazakhstan
MFA	Ministry of Foreign Affairs of the Republic of Kazakhstan
Laws and regulations	
AML/CFT Law	RK Law on Combating Legalization (Laundering) of Criminal Proceeds and Financing of Terrorism No.91-IV dated August 28, 2009
RK Law 88-VII	RK Law on Amendments and Modifications into Certain Legislative Acts of the Republic of Kazakhstan Pertaining to Introduction of Three-Tier Model of Division of Powers and Responsibilities of Law Enforcement, Prosecution and Judicial Authorities No.88-VII dated December 27, 2021
CC	Criminal Code of the Republic of Kazakhstan
CPC	Criminal Procedure Code of the Republic of Kazakhstan
PEC	Penal Enforcement Code of the Republic of Kazakhstan
CAO	Code of Administrative Offences of the Republic of Kazakhstan
CIVC	Civil Code of the Republic of Kazakhstan
COMC	Commercial Code of the Republic of Kazakhstan
CPC	Civil Procedure Code of the Republic of Kazakhstan
EAEU CRC	Customs Code of the Eurasian Economic Union
RK CRC	Customs Regulation Code of the Republic of Kazakhstan
Presidential Decree 203	RK Presidential Decree on Further Improvement of the State Governance System of the Republic of Kazakhstan No.203 dated November 11, 2019
Presidential Decree 428	RK Presidential Decree on Certain Issues Related to the Agency for Protection and Promotion of Competition of the Republic of Kazakhstan No.428 dated October 5, 2020
Presidential Decree 1271	RK Presidential Decree on Adoption of the Statute and Organizational Structure of the National Bank of the Republic of Kazakhstan No.1271 dated December 31, 2003
Constitutional Law	RK Constitutional Law on Astana International Financial Center No.438-V

438-V	dated December 7, 2015
Law 11-VI	RK Law on Payments and Payment Systems No.11-VI dated July 26, 2016
Law 105-V	RK Law on Pension Coverage in the Republic of Kazakhstan No.105-V dated June 21, 2013
Law 126-II	RK Law on Insurance Activities No.126-II dated December 18, 2000
Law 131-VII	RK Law on Amendments and Modifications in Certain Legislative Acts of the Republic of Kazakhstan Related to Combating Money laundering and Terrorist Financing and Government Price Control No.131-VII dated July 1, 2022
Law 142-II	RK Law on Non-Profit Organizations No.142-II dated January 16, 2001
Law 154-XIII	RK Law on Criminal Intelligence and Detective Operations No.154-XIII dated September 15, 1994
Law 155-I	RK Law on Notaries No.155-I dated July 14, 1997
Law 155-IV	RK Law on Commodity Exchanges No.155-IV dated May 4, 2009
Law 167-VI	RK Law on Foreign Exchange Regulation and Control No.167-VI dated July 2, 2018
Law 176-VI	RK Law on Legal Practice and Legal Assistance No.176-VI dated July 5, 2018
Law 202-V	RK Law on Permits and Notifications No.202-V dated May 16, 2014
Law 2155	RK Law of the National Bank of the Republic of Kazakhstan No.2155 dated March 30, 1995
Law 2198	RK Law on State Registration of Legal Entities and Record Registration of Branches and Representative Offices No.2198 dated April 17, 1995
Law 219-III	RK Law on Gambling Business No.219-III dated January 12, 2007
Law 2444	RK Law on Banks and Banking Activities No.2444 dated August 31, 1995
Law 300-III	RK Law on Export Control No.300-III dated July 21, 2007
Law 310-III	RK Law on State Registration of Ownership Titles to Real Estate Property No.310-III dated July 26. 2007
Law 410-V	RF Law on Combating Corruption No.410-V dated November 18, 2015
Law 413-IV	RF Law on Public Property No.413-IV dated March 1, 2011
Law 415-II	RK Law on Joint-Stock Companies No.415-II dated May 13, 2003
Law 416	RK Law on Combating Terrorism No.416-I dated July 13, 1997

Law 418-V	RK Law on Informatization No.418-V dated November 24, 2015
Law 461-II	RK Law on Securities Market No.461-II dated July 2, 2003
Law 474-II	RK Law on State Regulation, Oversight and Supervision of Financial Market and Financial Institutions No.474-II dated July 4, 2003
Law 498-V	RK Law on Postal Service No.497-V dated April 9, 2016
Law 510-II	RK Law on State Legal Statistics and Special Accounts No.510-II dated December 22, 2003
Law 56-V	RK Law on Microfinance No.56-V dated November 26, 2012
Law 78-II	RK Law on Financial Leasing No.78-II dated July 5, 2000
Law 94-V	RK Law on Personal Date and their Protection No.94-V dated May 21, 2013
Order 1009	Joint Order of the Designated Government Agency, Law Enforcement and Special Government Authorities No.1009 dated October 14, 2020
Order 265К	ARDFM Chairman's Order on Adoption of Methodology of Assessing the Degree of Exposure of Microfinance Organizations to Money Laundering and Terrorist Financing Risks No.265K dated September 13, 2021
Order 299К	ARDFM Chairman's Order on Adoption of Methodology of Assessing the Degree of Exposure of Professional Insurance Market Participants to Money Laundering and Terrorist Financing Risks No.299K dated September 30, 2021
Order 300К	ARDFM Chairman's Order on Adoption of Methodology of Assessing the Degree of Exposure of Professional Securities Market Participants to Money Laundering and Terrorist Financing Risks No.300K dated September 30, 2021
Order 317К	ARDFM Chairman's Order on Adoption of Guidance on Internal Procedures of Monitoring and Supervision of Banks, Large Shareholders of Banks, Financial Conglomerates and Institutions No.317K dated August 6, 2020
Order 938	Regulation on Provision by Obliged Entities of Information on Transactions that are Subject to Financial Monitoring adopted by Finance Minister's Order No.937 dated September 30, 2020
Order 13	The Order of the Chairman of Financial Monitoring Agency of the Republic of Kazakhstan No. 13 dated February 22, 2022