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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

MONEYVAL(2026)8

Anti-money laundering and counter-terrorist financing measures

Armenia

Sixth Round Mutual Evaluation Report

May 2026

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

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

Table of Contents

EXECUTIVE SUMMARY 4
ROADMAP OF KEY RECOMMENDED ACTIONS (KRA) 15
PREFACE 19
INTRODUCTION TO MONEY LAUNDERING AND TERRORIST FINANCING RISKS AND CONTEXT 20
CHAPTER 1. ASSESSMENT OF RISKS, CO-ORDINATION AND POLICY SETTING........ 34
CHAPTER 2. INTERNATIONAL CO-OPERATION 46
CHAPTER 3. FINANCIAL SECTOR AND VIRTUAL ASSET SUPERVISION AND PREVENTIVE MEASURES........ 59
CHAPTER 4. NON-FINANCIAL SECTOR SUPERVISION AND PREVENTIVE MEASURES........ 77
CHAPTER 5. TRANSPARENCY AND BENEFICIAL OWNERSHIP 92
CHAPTER 6. FINANCIAL INTELLIGENCE 103
CHAPTER 7. MONEY LAUNDERING INVESTIGATIONS AND PROSECUTIONS 119
CHAPTER 8. ASSET RECOVERY 132
CHAPTER 9. TERRORIST FINANCING INVESTIGATIONS AND PROSECUTIONS........ 143
CHAPTER 10. TERRORIST FINANCING PREVENTIVE MEASURES AND FINANCIAL SANCTIONS........ 151
CHAPTER 11. PROLIFERATION FINANCING FINANCIAL SANCTIONS 164
ANNEX A. TECHNICAL COMPLIANCE ANNEX 171
ANNEX B. TECHNICAL COMPLIANCE SHORTCOMINGS 257
GLOSSARY OF ACRONYMS 262

EXECUTIVE SUMMARY

1. This report summarises the anti-money laundering and countering the financing of terrorism (AML/CFT) measures in place in Armenia as at the date of the on-site visit 29 September - 10 October 2025. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Armenia's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

a) The authorities' understanding of risk is based on the NRA and is to some extent adequate, with some areas for improvement especially in relation to the impact of the foreign factor. The main ML threats identified stem from fraud, embezzlement, corruption, tax crimes, drug trafficking, and cybercrime.[1] The AT considers this conclusion as reasonable, especially when speaking about the domestic threat. ML and TF vulnerabilities and risks in relation to VAs need further analysis to ascertain the materiality of the sector and the reasonableness of a low TF risk of abuse through VAs. The national policies and strategies to address the ML and TF risks are satisfactory. The implementation of the National AML/CFT/CPF Strategy for 2025 to 2028 and the action plan are being monitored semi-annually, where the progress on implementation is discussed within the Interagency Committee. Some authorities showed how their own objectives and activities are largely consistent with the ML/TF risks identified in the 2024 NRA and with the actions envisaged in the AML/CTF National Strategy. National cooperation and coordination take the form of a case-by-case basis.

b) The legal framework for international cooperation is sound, and the country generally provides high-quality and timely assistance. The authorities have demonstrated that, in certain key complex ML cases, mostly related to corruption, they proactively seek assistance from foreign counterparts. However, this is not done on systematic basis with regard to other associated predicate offenses, such as drug trafficking. Overall, the LEAs and the FMC did not fully undertake a proactive approach to seeking intelligence from foreign counterparts. Mutual legal assistance is used to some extent for asset recovery, with two confirmed cases of seizure of illicit assets abroad. The financial supervisor demonstrated active cooperation with foreign regulatory authorities, while the cooperation by non-financial supervisors is limited, largely due to the domestic nature of the supervised entities.

c) Armenia has taken important steps to strengthen AML/CFT supervision of financial institutions and implement a risk-based approach since the last evaluation, including the introduction of cyclical on-site inspections during the latter part of the assessment period. The CBA has controls in place to prevent criminals from entering the regulated market through licensing requirements, though non-public investment funds and VASPs operated outside supervision for most of the assessment period until 2025 legislative amendments closed this gap. The banking sector received the highest supervisory attention and shows

[1] 2024 NRA, para. 185-186.

notable improvement in compliance, while smaller financial institutions display more limited understanding of risks and obligations.

d) The legal persons most frequently used in criminal activities are the LLCs, closed joint stock companies (JSCs), and, in some cases, non-profit organisations (NPOs).[2] All domestic legal persons must be registered with the State Registry. Basic information is publicly available and includes personal identification details, such as addresses, citizenship status, and birth/death records, along with company ownership, registration details, and tax status for businesses. The BO Registry is being gradually populated with BO data since 2021 but there are no verifications and checks on the accuracy of the BO data. The BO data is also held by FIs and the information kept therein is generally of a good quality, notwithstanding that deficiencies have been identified by the supervisors. The materiality of foreign legal arrangements does not appear to be significant. Administrative sanctions imposed do not appear as being dissuasive and effective, especially in view of the fact that the register is still half populated with the BO data.

e) The FMC has broad access to key datasets, including bank account registers, tax databases, criminal, and real estate records. While STRs are the main focus, the FIU also uses TTRs, requests, and open-source intelligence. Improving the volume and quality of STRs is essential for supporting competent authorities. Other agencies have timely access to relevant data, but LEAs lack direct access to the bank accounts registrar, which delays financial intelligence and adds pressure on the FMC. The FIU's resources are strained by many requests cantered on predicate offenses rather than money laundering. Intelligence bodies do not sufficiently look at the financial side of the investigation and outcomes often fall short of supporting ML hypotheses. Despite resource and software constraints, strategic analysis is effective, and the use of STRs and FIU notifications in ML investigations is showing positive growth.

f) Armenia's legal and institutional framework for identifying, investigating and prosecuting ML has undergone important changes in recent years. These reforms have led to an increase in the last two years in ML investigations and prosecutions, particularly in corruption-related cases. However, the system remains predominantly predicate-offence-driven, with a focus on self-laundering linked to domestic offences, while third-party and autonomous ML cases are not systematically pursued. Limited consideration is given by the LEAs to ML in connection with foreign or transnational organised crime, which impacts the type and scale of cases pursued. Prosecutions face delays and evidentiary challenges, and convictions to date remain few, involving small scale ML cases.

g) Significant efforts were also made towards establishing a legal and institutional framework for asset recovery as part of broader anti-corruption and anti-money laundering efforts. This led to the introduction of the NCBC regime which enhanced the country's ability to confiscate illicit assets. Asset recovery responsibilities remain dispersed among different agencies, with no overarching authority or cooperation framework to ensure a consistent and efficient approach. Overall, the results do not demonstrate that asset recovery of criminal proceeds is proactively pursued. Confiscation efforts are primarily focused on domestic proceeds. Measures taken against undeclared cross-border cash movements had

[2] 2024 NRA, par. 754

some results, including the application of fines, voluntary compensations and confiscations in smuggling related cases. However, there is no proactive approach to identifying potential indicators of proceeds of crime, including links to ML/TF. Armenia lacks a specialised assets management authority for seized and confiscated property, with responsibilities for asset management dispersed across various authorities.

h) Armenia has systems in place to identify, investigate and prosecute TF, and the relevant authorities are adequately trained and resourced. The authorities look for possible TF activity in all cases of suspected terrorism or from TF-related STRs. However, the use of funds raised through other forms of criminality for TF purposes and possible TF involvement in transactions linked to high-risk countries are insufficiently explored. The ability to identify TF is also limited by underreporting of suspected TF by the private sector. There have been no TF prosecutions or convictions to date, but there are no legal or procedural obstacles to prevent this or the imposition of appropriate sanctions in most cases. TF is integrated into counter terrorism strategies to some extent, and the authorities generally collaborate well on counter terrorism issues at both a strategic and operational level. There are alternative measures to TF convictions available to the authorities, although these have not been used in practice.

i) Armenia has established well-functioning frameworks for targeted financial sanctions related to terrorist financing (TF) and proliferation financing (PF), implementing UNSCR designations without delay. The country has demonstrated effective capacity to make designations under UNSCR 1373 for TF and has successfully identified and frozen assets under the Iran PF sanctions regime, with outcomes consistent with Armenia's low-risk profile. Armenia has robust systems in place for coordination and cooperation at a policy and an operational level for CPF. Banks and larger financial institutions demonstrate good understanding of TFS obligations with effective screening mechanisms, while smaller entities show more limited knowledge of sanctions evasion risks consistent with their domestic profiles and limited risk exposure.

Effectiveness & Technical Compliance Ratings

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

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

Risks and General Situation

1. Since the last evaluation round, Armenia has completed three NRAs: in 2017 based on data for the period 2014-2016 (2017 NRA), in 2021 based on data for the period of 2017-2020 (2021 NRA) and the 2024 NRA based on data covering 2021 to 2023. This last iteration of the NRA is based on a methodology developed by the Armenian authorities and includes an improved analysis of a broad range of risks that the country is facing with the highest focus on the vulnerabilities.

2. The main ML threats identified in the 2024 NRA stem from fraud, embezzlement, corruption, tax crimes, drug trafficking, and cybercrime. Compared to the 2015 MER findings, which indicated a lack of consensus among Armenian authorities regarding the most prevalent criminal activities for ML, now the perception is more unified. The ML residual risk level remained the same across all three iterations of the NRA.

3. The authorities concluded that the threat level related to TF is low, given that: (i) there were no favourable preconditions for terrorism and TF in Armenia, (ii) competent authorities effectively prevented attempts by individuals associated with terrorist organisations, (iii) criminal proceedings were initiated in four cases related to terrorism and the preparation of terrorism, which are not significant in terms of TF, (iv) Armenia's relations with high-risk countries that include money transfers, are limited to the natural ties it maintains with Armenian communities, and (v) no significant risks related to terrorism were identified and the hypothesis put forward regarding TF have been refuted.

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

4. Armenia has to be commended for actively engaging in efforts to continuously improve the understanding of the landscape of risks, by conducting three NRAs since the last evaluation round. The authorities' understanding of risk is based on the last NRA and is to some extent adequate, with some areas for improvement as described in the analysis below. The main ML threats identified stem from fraud, embezzlement, corruption, tax crimes, drug trafficking, and cybercrime.[3] The AT considers this conclusion as reasonable, especially when speaking about the domestic threat. A development from the previous MER is that the authorities have included an estimation of the magnitude and significance of the overall proceeds from criminal activity. The AT notes that according to the NRA, there has been no change in the threat level despite global dynamics in the ML/TF risk landscape in the last ten years, and the economic and demographic developments in Armenia post 2022.

5. The threat emerging from transnational organised criminal networks dealing in drug trafficking and other major crimes is considered as negligent. The authorities acknowledge the existence of large-scale drug trafficking cases, which have been considered for the NRA purposes, but remain of the view that this does not constitute a trend and typology in the Armenian context. The AT has concerns about the reasonableness of this conclusion and is of the view that the risk assessment should explore more the impact of the criminal activities carried out by transnational organised criminal groups.

6. TF risk was considered in all the iterations of the NRA and is considered to be low. The authorities reported that there is a separate TF risk assessment besides the section in the 2024 NRA, however the document was not made available to the AT due to high confidentiality nature of the data. To assess TF threats, the authorities considered conflicts driven by religious or ethnic movements, minority rights violations, extremist propaganda, the presence of terrorist organisations, instances of terrorism and TF, and connections with high-risk countries.

[3] 2024 NRA, para. 185-186.

7. At the policy making level, authorities are guided by the National Strategy on AML/CFT (2025-2028) and the Anti-Corruption Strategy (2023-2026). The implementation of the National AML/CFT Strategy and the action plan are being monitored semi-annually. Actions pertaining to supervisory authorities are not linked to higher materiality and risk areas, except for VAs.

8. The Interagency Committee serves as the authorized body responsible for national policy development and coordination of activities in the field of AML/CFT. The Committee proved to have valuable input when it comes to strategic coordination. Operational cooperation and coordination between competent authorities is not systemic and needs to be further strengthened.

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

9. Armenia has a sound legal framework enabling international cooperation on the basis of multilateral and bilateral agreements. The assistance provided is generally of good quality and effective. Overall, the global feedback on its quality and timeliness is positive. Since the last assessment, the authorities have taken steps to enhance the quality of the assistance provided to foreign counterparts and have adopted in some cases a more proactive approach to seeking information abroad.

10. The authorities have demonstrated that, in certain key complex ML cases, mostly related to corruption, they proactively seek assistance from foreign counterparts. However, with regard to other associated predicate offenses, such as drug trafficking, there are concerns that this is not done on a systematic basis. Mutual legal assistance is used to some extent for asset recovery, with two confirmed cases of seizure of illicit assets abroad.

11. LEAs and the FMC provide and to a various extent seek other forms of international cooperation in pursuing predicate offenses and ML using a wide range of channels. In particular, the FMC provides good-quality intelligence to its foreign counterparts in a timely manner and has demonstrated its ability to suspend transactions to secure proceeds of crime upon request from foreign counterparts. However, the authorities did not fully undertake a proactive approach to seeking intelligence from foreign counterparts.

12. The financial supervisor actively seeks and provides informal cooperation with foreign regulatory authorities in relation to fitness and propriety checks and supervisory activities. Cooperation by non-financial supervisors is more limited, although this is impacted by the domestic nature of the entities subject to supervision.

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

13. The CBA has controls in place to prevent criminals and their associates from entering the regulated market through a unified licensing approach across all financial institutions, with powers to reject or revoke licenses exercised when adverse information is identified and recent rules requiring annual re-evaluation of shareholders, beneficial owners, and managers. VASPs and non-public investment funds remained outside the supervisory regime until a new regulatory framework was adopted in 2025.

14. The CBA demonstrates comprehensive understanding of ML/TF risks across the financial sector, assessing risks for core financial institutions through a structured model combining systemic and institutional elements supported by extensive data collection, while smaller entities are assessed through supervisory judgement. AML/CFT supervision is guided by dedicated procedures and methodologies introduced gradually from 2020, prescribing permanent off-site risk analysis and compliance scrutiny for all material sectors, with more in-depth on-site inspections recently introduced based on ML/TF risk,

though for much of the assessment period inspections were triggered by specific events or took the form of sectoral thematic reviews

15. Most banks demonstrate good understanding of risks relevant to their operations, while other FIs refer to broader national threats with limited understanding of how these materialise in their business context, and the distinction between ML and TF risks remains weak across the sector with most entities assessing TF threat as low. All FIs demonstrate awareness of their AML/CFT obligations and have internal controls in place, though STR reporting levels remain relatively modest with entities applying a high threshold for identifying suspicious activity. The CBA actively engages in supervisory outreach providing structured feedback and has demonstrated improved ability to impose proportionate sanctions including fines, license revocations, and removal of managers.

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

16. Market-entry controls for higher-risk DNFBPs including casinos, online gambling operators, notaries, and advocates are in place through licensing or registration regimes, though analysis does not always include beneficial ownership verification and controls for other DNFBPs remained largely absent during the assessment period.

17. Supervision of the gambling sector by the SRC reflects a general understanding of ML/TF risks aligned with the NRA but lacks a structured risk-based methodology and relies largely on ad hoc triggers, while supervision of notaries by the Ministry of Justice (MoJ) remains limited and constrained by resources despite adopting a basic risk-assessment methodology in late 2023. AML/CFT supervision of advocates is absent, as the Chamber of Advocates (ChoA) considers attorney-client privilege to preclude such oversight, with no inspections conducted during the assessment period. Since assuming supervisory functions in 2023, the FMC has made significant progress in establishing an AML/CFT supervisory framework despite very limited resources, moving from ad-hoc identification of reporting entities to conducting risk assessments and providing feedback with particular emphasis on higher-risk sectors such as real estate agents.

18. Understanding of ML/TF risks and AML/CFT obligations varies widely across DNFBPs: casinos and gambling operators demonstrate the strongest understanding and apply relatively robust controls, while smaller DNFBPs have less developed understanding, with most having little knowledge of obligations before supervisory engagement intensified in 2023. The use of sanctions and remedial measures has been limited and uneven across DNFBP sectors and has not demonstrated a consistent or sufficiently dissuasive effect, with the exception of some recent enforcement action in the gambling sector, and no AML/CFT-related measures were applied to advocates while disciplinary actions in relation to notaries have been modest.

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

19. Armenia carried out the risk assessment of domestic and foreign legal persons (all), and of legal arrangements and concluded that the most vulnerable are the LLCs, JSCs and the NPOs in certain cases. The indicators used are all relevant, with additional scope for analysis needed in assessing the rationale of having domestic and foreign legal persons with no relationship with a reporting entity. Armenia does not recognise trusts and similar legal arrangements and its’ exposure to foreign legal arrangements as low.

20. The State Register Agency maintains the State Registry which holds basic information on the Armenian legal persons and where available, BO information. Law enforcement and supervisory

authorities have direct access to the State Registry which allows for accessing adequate, accurate, and up-to-date basic information, and when available, BO information.

21. A multi-pronged approach to access BO data is used through three main sources: (i) information held by the reporting entities, mostly banks; (ii) information contained in the State Registry, and (iii) information held by the legal persons. Effectiveness of the multi-pronged approach would benefit from further development given that the State Registry is not yet fully populated, and the absence of a legal requirement for legal persons to have a bank account. LEAs do not have direct access to reporting entities' information but can access it through a court order or through the FMC.

22. During 2021 to 2024 1,903 administrative proceedings were initiated against legal persons, of which nine were for incorrect or incomplete information, and the rest for failure to submit BO information to the State Registry. Of these, 39% led to remediation measures, which is a positive outcome. In the rest of the cases, the imposed sanctions (mainly warnings) do not appear to be neither dissuasive nor effective.

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

23. In recent years, the Armenian FIU has significantly expanded its human and IT resources. It collects STRs, threshold-based disclosures, cash declarations, and reports on non-disclosure of cash at borders for both operational and, to a lesser extent, strategic analysis. While banks are the predominant reporting sector, overall STR submissions remain insufficient, especially among DNFBPs. STRs from financial institutions generally contain relevant information consistent with the primary ML/TF risks highlighted in the NRA, though some sectors, such as drug trafficking, are exceptions.

24. The FIU supports LEAs with financial intelligence for investigative purposes, and LEAs consider the quality of FIU information to be high. Strategic analysis also benefits other authorities. However, intelligence agencies, frequently request information from the FIU, mostly relating to predicate offenses rather than ML. Processing these requests, often requiring input from foreign partners and reporting entities, has strained FIU resources.

25. Authorities securely share financial intelligence, and the FIU actively coordinates with them through committees, joint teams, and bilateral meetings, underpinned by MoUs. The FIU's IT framework and safeguards ensure data confidentiality.

26. Armenia's legal and institutional framework for identifying, investigating and prosecuting ML has undergone important changes in recent years. This included the revision and the responsibilities of the relevant LEAs involved in intelligence-gathering and investigations into ML and associated predicate offences. Progress in anti-corruption reforms has strengthened the anti-corruption institutional framework, notably through the establishment of specialised institutions and courts. These developments have contributed to an increase in ML investigations and prosecutions over the last two years and positively impacted the pursuit of corruption-related ML cases, including high-profile ones. However, the system remains predominantly predicate-offence-driven. Most ML investigations are initiated in the context of predicate offences investigations, while other potential sources for ML cases such as MLA requests, foreign intelligence and cash seizures remain underutilized. There has been a recent increase in the number of ML investigations stemming from FMC disseminations, which is a positive development. Nevertheless, there is still insufficient proactive use of both domestic and foreign intelligence. The number and the characteristics of ML investigations and prosecutions are yet not fully in line with the overall level risk, considering the limited risk understanding of ML relating to foreign predicated or transnational crime. This impacts the type and the scale of cases pursued.

27. The focus remains on self-laundering cases linked to domestic predicates, while third-party and autonomous ML cases are not systematically pursued. No investigations have been initiated against legal persons, despite indications that legal persons are frequently involved in ML and associated offences. Prosecutions are following the investigations trend but are often prolonged, hindered by evidentiary challenges and procedural delays.

28. There are few examples of complex, internationally linked ML cases for which the authorities are commended. However, no convictions reflect such profile. The few convictions achieved during the period under review involve small-scale self-laundering cases associated with fraud, which is not in line with the country's risk profile and does not feature the characteristics of an effective system. Alternative criminal measures have not been pursued by the country.

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

29. Armenia's legal and institutional framework for identifying, investigating and prosecuting ML has undergone important changes in recent years. This included the revision and the responsibilities of the relevant LEAs involved in intelligence-gathering and investigations into ML and associated predicate offences. Progress in anti-corruption reforms has strengthened the anti-corruption institutional framework, notably through the establishment of specialised institutions and courts. These developments have contributed to an increase in ML investigations and prosecutions over the last two years and positively impacted the pursuit of corruption-related ML cases, including high-profile ones. However, the system remains predominantly predicate-offence-driven. Most ML investigations are initiated in the context of predicate offences investigations, while other potential sources for ML cases such as MLA requests, foreign intelligence and cash seizures remain underutilized. There has been a recent increase in the number of ML investigations stemming from FMC disseminations, which is a positive development. Nevertheless, there is still insufficient proactive use of both domestic and foreign intelligence. The number and the characteristics of ML investigations and prosecutions are yet not fully in line with the overall level risk, considering the limited risk understanding of ML relating to foreign predicated or transnational crime. This impacts the type and the scale of cases pursued.

30. The focus remains on self-laundering cases linked to domestic predicates, while third-party and autonomous ML cases are not systematically pursued. No investigations have been initiated against legal persons, despite indications that legal persons are frequently involved in ML and associated offences. Prosecutions are following the investigations trend but are often prolonged, hindered by evidentiary challenges and procedural delays.

31. There are few examples of complex, internationally linked ML cases for which the authorities are commended. However, no convictions reflect such profile. The few convictions achieved during the period under review involve small-scale self-laundering cases associated with fraud, which is not in line with the country's risk profile and does not feature the characteristics of an effective system. Alternative criminal measures have not been pursued by the country.

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

32. Armenia has made significant efforts towards establishing a legal and institutional framework for asset recovery as part of its broader anti-corruption and anti-money laundering efforts. Through successive Anti-Corruption Strategies and dedicated AML/CFT/PFT policies, the civil confiscation regime has been established, a specialised department have been created within the GPO, and implementation mechanisms have started to take shape. However, the results obtained in terms of seizures, confiscations, are not fully

convincing that asset recovery is proactively pursued as a policy objective in all ML and proceeds generating cases.

33. Asset recovery responsibilities remain dispersed among different agencies, each acting largely within the jurisdiction of their own investigations. While the GPO is tasked with coordinating civil confiscation, there is no overarching authority or cooperation framework to ensure a unified, efficient, and consistent approach to asset tracing, seizing, and confiscation across different types of cases. The FMC has the power to suspend transactions or business relationships, which contributes to securing criminal property, but this power is rarely used.

34. The results do not demonstrate asset identification and tracing is systematically pursued in pre-trial investigations. Particular difficulties are noted in tracing crypto assets. The confiscation efforts are primarily focused on recovering the proceeds of domestic predicate crimes within the jurisdiction. There are no examples of successful asset recovery from foreign jurisdiction, although asset seizure has been applied in two cases. Overall, a positive assessment of the asset recovery system cannot be made, including due to the lack of comprehensive, reliable, and analysed data. Notwithstanding, the introduction of the NCBC regime has enhanced the country's ability to confiscate illicit assets.

35. Measures taken against undeclared cash movements and associated crimes, such as smuggling, resulted in fines, voluntary returns and confiscations. However, there is no proactive approach in identifying and analysing false or non-declarations of cash and BNIs, including systematically assessing any indicators of proceeds of crime and their potential link to ML/TF.

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

36. Armenia has the necessary institutional framework for the identification, investigation and prosecution of TF and the relevant authorities are adequately trained and resourced. Appropriate steps are taken to identify possible TF activity from terrorism investigations and STRs related to TF. However, the use of funds raised through other forms of criminality for TF purposes and possible TF involvement in transactions linked to high-risk countries are not sufficiently explored. The ability to identify TF is also limited by underreporting of suspected TF by the private sector.

37. There has been one TF investigation during the assessment period, some aspects of which are ongoing, and no TF prosecutions or convictions to date. Notwithstanding, in most respects, the necessary sanctions are available under the legal framework and the prosecutors, and the courts have the necessary resources to deal with TF cases.

38. TF is integrated into counter terrorism strategies but overall, there is scope for a greater focus on TF at a national level. The authorities generally collaborate well on counter terrorism issues, but there is scope for greater sharing of information and intelligence to support counter-terrorism efforts. Armenia has measures in place that could be used as alternatives to TF convictions, although they have not been used in practice.

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

39. Armenia's framework for targeted financial sanctions (TFS) related to TF is well developed and implemented without delay, with UNSCR designations becoming immediately effective in domestic law and the FMC promptly communicating updates primarily to banks, while other reporting entities rely on voluntary subscription or independent monitoring of UN lists via the FMC website. Armenia has

demonstrated capacity to implement designations under UNSCR 1373 swiftly, with no assets frozen under TF-related UNSCRs consistent with the country's low-risk profile.

40. The NPO sector has been identified and assessed as low TF risk with robust financial controls in place, though mitigating measures are not risk-based, and oversight of compliance was absent for most of the assessment period; a framework for targeted oversight of higher-risk NPOs was introduced towards the end of the assessment period but has not yet been implemented.

41. Banks and larger financial institutions demonstrate good understanding of TFS obligations with effective screening mechanisms confirmed through thematic inspections. Smaller financial institutions and DNFBPs appropriately rely on manual checks given their simple, domestic client base and limited risk exposure, though understanding of sanctions evasion remains less mature among these entities. Supervisory engagement with banks is robust and includes regular testing of TFS controls, while supervision of non-bank financial institutions and DNFBPs remains more limited and focuses mainly on screening obligations rather than broader sanctions evasion risks

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

42. Armenia has established well-functioning mechanisms for proliferation financing (PF) policy coordination through the Interagency Committee and FMC, ensuring structured cooperation and information exchange, and has completed two PF NRAs demonstrating a generally sound understanding of PF risks, including links to PF-hub jurisdictions and sanctions-evasion typologies, though analytical gaps exist in the NRA reports regarding financial flows and virtual assets despite more developed practical understanding of these issues.

43. PF-related targeted financial sanctions are implemented without delay following the same mechanisms as TF-related TFS, with Armenia demonstrating its capacity to identify and freeze assets promptly under the Iran PF sanctions regime.

44. Banks and larger financial institutions have conducted PF risk assessments and demonstrate good understanding of PF-TFS obligations and evasion risks with effective compliance mechanisms in place. Smaller financial institutions and DNFBPs show more limited knowledge of PF risks, which is consistent with their domestic profiles and lower risk exposure, though they have appropriately carried out risk assessments. Supervisory engagement mirrors the TF-TFS approach with guidance, outreach, and inspections contributing to overall compliance, and the CBA monitors risk assessments put in place by financial institutions, though supervisory focus on specific PF sanctions evasion issues remains limited among non-bank financial institutions and DNFBPs.

ROADMAP OF KEY RECOMMENDED ACTIONS (KRAs)

1. Armenia underwent a Mutual Evaluation of its anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place during its on-site visit to the country from 29 September – 11 October 2025. This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology.
2. The Mutual Evaluation Report identifies the strengths and weaknesses of Armenia's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) are included in this KRA Roadmap.
3. The following presents the KRA Roadmap for the Republic of Armenia as adopted by MONEYVAL Plenary in May 2026. Based on Effectiveness and Technical Compliance Ratings, Armenia is placed in enhanced follow-up. This KRA Roadmap also serves as the basis for Armenia's follow-up process.

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

a) Armenian authorities should take action to deepen the national ML risk understanding by including other sources of information such as the incoming international requests (formal and informal) by predicate offence, and typologies of cross-border and organized crime concerning relevant predicate offences such as drug trafficking. The authorities should re-examine the impact of the foreign ML threats and the overall impact on the overhaul ML risk of Armenia. Proportionate mitigating measures should be taken at a national level.

b) Authorities should distinguish between ML and TF threats, vulnerabilities, and residual risks for FIs and DNFBPs by products and services. For VAs, a more comprehensive analysis of potential TF risk of abuse is needed (for example, using international reports, estimating the activity of VASPs on the national territory, estimating the VAs turnover, sectors where VAs are particularly used, etc.). Proportionate mitigating measures at a national level should be subsequently taken.

IO.2 (International co-operation)

N/A

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

c) The CBA should complete the first full cycle of risk-based on-site inspections, covering the entire population of each FI type within the prescribed timeframes and make stronger use of the extensive data it collects to guide targeted, risk-driven inspections.

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

d) Armenia should introduce registration or licensing requirements for all DNFBPs under FMC supervision to ensure full supervisory visibility and enable effective market-entry controls. These regimes should include fit-and-proper requirements, encompassing criminal background checks and verification of BO, and the FMC should be provided with legal powers to refuse, suspend, or revoke authorisations where individuals or entities are found unfit.

e) Armenia should prioritize operationalization of the new Operating Centre and ensure continuity of AML/CFT supervision of gambling operators during the transition. The SRC should develop and implement a risk-based supervisory methodology for the gambling sector, supported by adequate tools and sector-specific data.

f) Armenia should establish effective AML/CFT supervision of advocates, including implementation of risk-based framework with inspections and dissuasive sanctions.

IO.5 (Transparency and beneficial ownership)

g) Authorities should enhance their understanding on domestic and foreign legal persons' vulnerabilities of (i) not having a fully populated BO registry, (ii) absence of checks on the accuracy of the BO information, (iii) rationale of having legal persons with no relationship with a reporting entity, and (iv) TF geographic vulnerabilities considering the residency of the BOs/founders and the country of registration of BO/founder.

h) The State Register Agency should carry out systemic verification checks of the accuracy and relevance of BO information on a risk-based approach, to ensure its reliability and mitigate the risks of the creation of legal persons for ML/TF purposes.

IO.6 (Financial intelligence)

i) The intelligence bodies (NSS, MIA, SRC, ACC in the intelligence capacity), as primary recipients of FMC disseminations, and as responsible authorities for initiating ML cases, should focus more on the ML aspect in their intelligence gathering activities. Specialised officers should be trained on systematically developing and using financial intelligence and tracing criminal proceeds related to ML/FT.

IO.7 (Money laundering investigations and prosecutions)

j) Armenia should take measures to actively pursue the investigation and prosecution of ML, particularly of complex third-party and autonomous ML cases, and ensure that all relevant sources are fully utilised for potential ML identification, with appropriate consideration to be given to all potential foreign or transnational links. The country should take measures to ensure that convictions are secured in all types of ML cases and that the sanctions applied are effective, proportionate and dissuasive.

k) Armenia should ensure that the interpretation and understanding of ML offence by Courts in relation to the purposive element of certain acts of ML, does not impede prosecution of ML cases in line with international standards.

l) The authorities should review the investigative bodies' access to financial information for evidentiary purposes, ensuring that they can obtain all information necessary for investigations and prosecutions of ML and associated predicate offences, even in the absence of a direct link to or control by the suspect or the accused, in order to facilitate the identification of the extent of criminal networks and/or the scale of criminality, in particular in third-party or autonomous ML cases.

IO.8 (Asset recovery)

m) The country should take stock of the overall asset recovery regime at all stages (identification, tracing, seizing and confiscating) to identify the challenges in achieving results aligned with the estimated volume of criminal proceeds and the country risk profile. Subsequent strategic and policy measures should be taken to enhance the institutional framework, provide sufficient guidelines and adequate resources to LEAs on asset recovery matters.

n) Armenia should put in place a system of management of seized property to preserve its value.

o) The country needs to invest in building expertise and resources for tracing, seizing, and confiscating assets. This includes providing law enforcement agencies with the tools, training, and technical expertise to effectively pursue parallel financial investigations and apply provisional measures.

IO.9 (Terrorist financing investigations and prosecutions)

p) The authorities should be provided with training and guidance on identifying possible TF and terrorist assets from cases involving criminality other than terrorism.

q) Guidance or other outreach focused on TF should be provided to reporting entities to enable them to identify and report possible TF activity.

r) The NSS and the IC should put in place procedures or other measures to ensure that possible TF involvement in transactions to high-risk countries are routinely explored.

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

N/A

IO.11 (Proliferation financing financial sanctions)

N/A

PREFACE

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

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

The evaluation was conducted by an assessment team consisting of:

- Alexandra POPA, Financial Analyst, Financial Supervisory Authority, Romania
- Kate RABEY, Crown Advocate, Counsel to the Law Officers, International Standards and Criminal Justice Policy, Law Officers of the Crown, Guernsey
- Pauline SALIBA, Executive Secretary of National Coordinating Committee on Combating Money Laundering & Funding of Terrorism, Malta
- Michal SZERMER, Director in the Department of Financial Information, Ministry of Finance, Poland
- Mikko VÄRRI, Head of Financial Intelligence Unit, Finland

with the support from the MONEYVAL Secretariat of Irina TALIANU, Kotryna FILIPAVICIUTE, Stela BUIUC, Fadma BOUHARCHICH, Maria GORECKA.

The report was reviewed by Michelle MORALES (United States of America), Michael ADAMBERRY (Gibraltar) and FATF.

Armenia previously underwent a Mutual Evaluation in 2015, conducted according to the *2013 FATF Methodology*. The 2015 evaluation and the 2018 follow-up report have been published and are available at MONEYVAL website.

That Mutual Evaluation concluded that the country was compliant (C) with Recommendations 9, 11, 13, 14, 15, 16 17, 18, 19, 20, 21, 23, 27, 29, 32, 33, 34, 40; largely compliant (LC) with Recommendations 2, 3, 4, 5, 6, 8, 10, 22, 24, 25, 26, 30, 35, 36, 37, 38, 39; partially compliant (PC) with Recommendations 1, 7, 12, 28, 31; and had no non-compliant (NC) rating.

Based on these results, Armenia was placed in regular follow-up. Since its last evaluation, Armenia achieved three technical compliance re-ratings:

- 2 Recommendations upgraded from PC to LC
- 1 Recommendation upgraded from LC to C

In total, 3 Recommendations (R.12, R.28, and R.31) remain rated PC since the last evaluation.

Introduction To Money Laundering and Terrorist Financing Risks and Context

1. Located in the South Caucasus region of Eurasia, Armenia is a landlocked country with a total area of 29,743 square kilometres. Armenia shares borders with Türkiye in the west, Georgia in the north, Azerbaijan in the east and Iran in the south. The population of Armenia is 2.99 million.[4] Armenian authorities estimate that about 7 million Armenians live outside the country. Yerevan is the largest city and the country's capital. Armenia is a small open economy with a Gross Domestic Product (GDP) of 24.4 billion euros (EUR).[5] The national currency is the Armenian Money Dram (AMD).

2. Armenia is a unitary parliamentary democratic republic. Under the current Constitution, the President serves as head of state, while executive authority is vested in the Government, led by the Prime Minister. Since 1995, the legislative power is vested in the National Assembly, which is a unicameral parliament composed of at least 107 members elected for a five-year term. Armenia's legal system is based on civil law. In Armenia, the judiciary consists of the Constitutional Court, Court of Cassation, Courts of Appeal, Courts of First Instance of General Jurisdiction, Administrative Court, Anti-Corruption Court and Bankruptcy Court.

3. Armenia is a member of the United Nations (UN), the Council of Europe (CoE), the European Bank for Reconstruction and Development, the Organisation for Security and Cooperation in Europe, the World Bank, the International Monetary Fund (IMF), Interpol, and the Egmont Group of Financial Intelligence Units. Armenia signed a strategic co-operation agreement with Europol in 2021. The country is a member of the Eurasian Economic Union since 2015.

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

Overview of ML/TF/PF Risks

4. Armenia's ML/TF/PF risk profile is primarily shaped by domestic predicate offences, while cross-border crimes and sector-specific vulnerabilities also contribute to overall risk. Taking into account the identified threats and vulnerabilities, Armenia assesses its residual ML risk as medium, whereas TF and PF risks remain low. The expanding activity of VASPs[6] and use of crypto assets creates heightened ML vulnerabilities, as such services have been used to launder proceeds of crime.

5. The crimes representing the highest ML threats in Armenia are fraud, corruption (embezzlement, abuse of official power), tax evasion, drug trafficking, and cybercrime. Between 2021 and 2023, the total amount of damage identified during the investigation of criminal cases, including the proceeds of crimes established by convictions, and the proceeds tied to claims for the confiscation of illegal property and settlements amounts to approximately EUR 1.6 billion, or about 2.72% of the country's average annual GDP.

6. Cross-border crimes include the smuggling of cash, monetary funds, and payment instruments, cultural values and raw materials of strategic importance, military products, equipment, firearms, and other materials, as well as narcotic drugs, psychotropic substances, their analogues, derivatives, or precursors, involving abuse of official powers. According to the authorities, the main ML threats in

[4]. World Bank data, 2023.
[5]. National statistics.
[6] Armenian legislation uses the terms "crypto-assets" and "crypto-asset service providers" to refer to what the FATF standard defines as virtual assets (VAs) and virtual asset service providers (VASPs). For purposes of this report, the FATF terminology is adopted throughout.

Armenia are domestic, while cross-border predicate offenses having only a limited impact on the country's overall ML risk exposure.

7. There are no active terrorist groups in Armenia, nor have there been any reported extremist propaganda or violations of minority rights. No nationals or residents appear on UN Security Council sanctions lists, and no terrorist financing cases have been recorded. The overall TF risk in the country is assessed as low.

8. Armenia is not a significant producer of controlled or military goods and technologies. No permits have been issued for exports of dual-use goods to the Islamic Republic of Iran and the Democratic People's Republic of Korea, and no criminal cases related to proliferation financing or weapons of mass destruction have been initiated. Following the re-establishment of sanctions against Iran in September 2025, reporting entities have identified matches with persons designated for PF under the relevant UN sanctions regimes and applied freezing measures in accordance with the applicable legal framework.

9. In the financial sector, risks are primarily associated with servicing a small segment of non-resident and offshore clients. The percentage of non-resident customers is low, with approximately 98% of all financial institutions' clients being resident natural or legal persons. While cross-border transfers to higher-risk countries have increased, the authorities estimate this is largely driven by Armenian diaspora presence in those regions. Due to an increase of the number of VASPs, the growing volume of associated transactions, as well as the fact that their services are at least partially used for the purpose of laundering allegedly illicit funds, the risks associated with crypto assets are perceived as high.

10. In the non-financial sector, casinos do not issue certificates of winnings, reducing certain ML risks. However, online gambling accounts have been used to launder fraudulent funds. The proportion of foreign customers has decreased from 2.5% to 1.1%. While the number and value of large transactions and reports to the FMC have increased, STR volumes remain low, indicating need for continued supervisory efforts. Real estate sector is exposed to the risks of laundering proceeds of crime especially derived from corruption. While authorities estimate that most purchases involve residents, notaries often face challenges in identifying the sources of funds and beneficiaries in transactions.

11. Since the 5th round evaluation of Armenia's AML/CFT system, the list of threats has evolved. Consequently, threats now stem from crimes related to fraud, corruption, drug trafficking, tax evasion and cybercrime, including those committed via new technologies using cryptographic assets.

Country's risk assessment & Scoping of Higher Risk Issues

12. Since the last evaluation round, Armenia has completed three NRAs: the 2017 NRA (based on data for the period 2014-2016), the 2021 NRA (based on data for the period of 2017-2020), and the most recent, the 2024 NRA (covering the period of 2021 to 2023).

13. The 2024 NRA concluded that the risk level for TF is low. The NRA substantiates this conclusion with the fact that no terrorism offences have been committed in the country, and its ethnic homogeneity due to which there are no ethnically or religiously motivated conflicts.

14. The areas of enhanced focus by the assessment team (AT) were banking sector, real estate sector, relationship with high-risk countries, corruption, drug trafficking and organised crime related ML, as described below.

15. <u>Banking sector:</u> The financial sector is dominated by banks that hold 83% of the total financial system assets. The 2024 NRA estimates that nearly 20% of the banking clients use high-risk products, such as personal banking services, and establish business relationships non-face to face; 18.6% of the banking clients are walk in customers (data of 2023). According to the 2024 NRA, the proportion of

high-risk clients, including non-resident clients and those from high-risk jurisdictions, has increased, although the overall share remains low at 4.25%. The share of cross-border transfer of funds featured in the STRs filed by banks has increased as well, as described above. The AT focused on the adequacy of preventative AML/CFT measures in the banking sector in line with the country risks and institutional risk exposure. The AT examined the Central Bank of Armenia approach to assessing sectorial and institutional risks of the banking sector and the effectiveness of the risk-based AML/CFT and TFS supervision. Given the importance of foreign ownership in the Armenian banks (58% as of 2023) and Law on Cashless governance related controls, including the suitability of checks intended to prevent criminal behaviour.

16. Real estate sector: Although the overall value of the real estate transactions is not known, the Armenian authorities estimate that non-residents account for approximately 8-10% of total real estate transactions. The MONEYVAL mutual evaluation report of 2015 highlighted that the risks associated with the real estate sector stemmed from the use of cash for the real estate purchases. Although the 2024 NRA indicates that this proportion has decreased, it does not provide any supporting evidence, such as specific quantitative data, to substantiate this claim. The implementation of the Law on Cashless Transactions is expected to reduce the risk. According to the 2024 NRA, the sector's risk level is the highest among non-financial institutions. The AT focused on the application of the preventative measures by relevant stakeholders involved in real estate deals: real estate agents, notaries, banks and other legal professionals (as applicable) that prepare for or carry out transactions for their clients concerning buying and selling of real estate.

17. Corruption: Armenia has made positive progress in anti-corruption reforms[7], including through policy development, legislative advancements, and strengthening of its the anti-corruption institutional framework. Over the period 2019-2022, large-scale investigations were initiated against high-level corruption and kleptocratic networks connected to previous regimes. However, these cases remained ongoing with no convictions secured[8]. The latest assessment of the country's anti-corruption efforts caried out by Organisation for Economic Co-operation and Development (OECD) highlights progress in several areas but also indicates a slight decline in the independence of the judiciary and specialised anti-corruption bodies, and a limited progress in relation to the independence of the prosecution service. The AT considered: (i) the outcomes of the initiated large-scale investigations in relation to high-level corruption and whether the ML aspect was identified and addressed ; (ii) the overall capacity of law enforcement authorities (LEAs) to detect and effectively investigate and prosecute ML cases related to corruption and confiscate corruption proceeds; and iii) whether the preventive measures and controls related to politically exposed persons (PEP) are adequate and effective.

18. Organised crime-related ML: The country's assessment of risks related to organised crimes is limited to domestic organised crime, concluding on an overall insignificant ML threat. The potential threats posed by transnational organised criminal groups are not comprehensively explored. However, there are indications[9] that this area requires greater attention, particularly considering Armenia's strategic location at the crossroad of the Middle East, Europe and Asia, which increases its exposure to organised crime.

19. Concerning drug trafficking, Armenia lies on a key trafficking route through the South Caucasus, serving as a transit country for narcotics originating from Afghanistan and Iran and destined for

[7] Armenia: Fifth round of anti-corruption monitoring follow-up report, OECD (2025).

[8] Council of Europe's Group of State against Corruption (GRECO) on Armenia (2024).

[9] United States Department of State Bureau of International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report, Volume 1, March 2022, p. 81 https://www.state.gov/wp-content/uploads/2022/03/22-00767-INCSR-2022-Vol-1.pdf; Illicit Financial Flows and Asset Recovery in the Republic of Armenia, UNICRI (2021). source : https://www.eeas.europa.eu/delegations/armenia/illicit-financial-flows-and-asset-recovery-republic-armenia_en

European and Russian markets. Although the country is not a major global hub, its role remains notable due to the geographic proximity to Iran, established smuggling networks, and continued trafficking through key border crossings such as Meghri. Whilst stronger anti-drug trafficking measures have resulted in an average of 46,6% increase in drug seizures over the past five years, significant quantities of narcotics are still estimated to enter the jurisdiction from the neighbouring and other countries, which informed AT focus on the authorities' efforts to detect and pursue ML associated with drug trafficking.

20. Relationship with high-risk jurisdictions**:** Armenia and Iran have long maintained political, economic, and diplomatic ties, shaped by geographic proximity and mutual interests, with a multifaceted trade relationship, supported by bilateral and multilateral agreements. The Iran-Armenia chamber of commerce was established in Tehran in 1993. In February 2024 Armenian authorities signed a Memorandum of Understanding with Iran, following the 18th meeting of the Iran-Armenia Joint Economic Committee, with media reporting plans expand cooperation in several areas, including trade, customs, maritime transportation, food and medicine. An Iranian Trade Centre in Yerevan was inaugurated in 2024, intended to activate the North-South Corridor and as entry into the Eurasian Union market. As a member of the Eurasian Economic Union (EAEU), Armenia is part of the free trade agreement (set to take effect in May 2025) between the EAEU and Iran, which aims to reduce tariffs and enhance trade between Iran and EAEU member states.

According to the 2024 NRA, financial flows from and to Iran relate mainly to imports and exports between the two countries. Notwithstanding, one Iranian bank with a presence in Armenia is subject to OFAC sanctions and has maintained correspondent banking relationship with its parent company in Iran. The AT focused on the risks associated with economic relations with Iran, given the latter's structural failings in the fight against ML/TF and the threat this poses to the international financial system. Additionally, the AT focused on ties (direct and/or indirect) with other heightened risk jurisdictions.

21. Several areas that warrant a reduced focus due to low ML/TF risk and materiality are life and other investment linked insurance services (no such services exist) and mandatory pension funds (early withdrawals are possible under strictly limited circumstances, such as in the case of a serious disease, disability, or for foreign employees - return to their home countries).

Materiality

22. Armenia's GDP reached EUR 24.4 billion in 2024. In previous years, it stood at EUR 22.9 billion (2023), EUR 20.5 billion (2022), EUR 16.8 billion (2021), and EUR 14.9 billion (2020). Following a contraction in 2020 due to the COVID-19 pandemic, the economy rebounded, with GDP growth of 5.8% in 2021, 12% in 2022, and 8.3% in 2023 (World Bank data). The primary drivers of this growth have been the stable expansion of the services sector and trade, reflecting the economy's underlying potential. Since 2022, growth has also been supported by additional capital and labour inflows, money transfers, and re-exports linked to regional geopolitical developments.[10] Poverty and unemployment have declined over this period to 24.8% and 12.6%, respectively.

23. In Armenia, the largest GDP generating components are trade (wholesale and retail), financial services, construction and manufacturing. According to the NRA, the Russian Federation accounted for about 35% of Armenia's total trade turnover during the period 2021-2023, while EU countries contributed around 15% with Germany being the primary trade partner; Armenia has also significant trade relations (import) with China, Georgia and Iran which were main trading partners (importers) in 2024. Imports from and exports to Iran respectively amount to approximately EUR 588 million and EUR 90.8 million in 2023, according to the 2024 NRA. Fluctuating trends with other elevated risk

[10]. World Bank. Armenia Public Finance Review - Enhancing Fiscal Policy Efficiency (2024), p. 2 and p. 22.

jurisdictions such as Iraq, Syria and Lebanon are observed, albeit Armenian authorities estimate that the level of turnover remains comparatively low.[11]

24. At the end of 2024, Armenia's banking sector was composed of 18 domestic banks (with EUR 26.6 billion in assets), 4 of which had foreign BOs, while 5 have BOs of dual citizenship (Armenian and foreign). Armenian authorities estimate that the ratio of high-risk customers in the banking sector has increased from 1.5% to 4.25% between 2021 and 2023.

25. In Armenia, the financial system is dominated by banks, holding over 83% of market assets, with lower ML/TF risks in sectors like mandatory pension funds and insurance, while emerging risks are found in the securities market, electronic payment services, and high-risk non-financial entities like online gambling operators.

Financial sector, VASPS and DNFBPs

26. An overview of the financial sector and designated non-financial business and professions (DNFBPs) is provided in the tables below. At the time of the on-site visit, no virtual asset service providers (VASP) were registered or licensed in Armenia.

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

A- Type of Entity - to be listed in descending order of size	B- Type of Entity - to be listed in descending order of size	C- Number registered or licensed	D – Explanation for order of listing	E – Market size EUR
Banks	18	18	Based on the results of National/Sectorial risk assessments and market share	26,662,348,612
Entities Engaged in Money (currency) Transfer Services[12]	14	14		265,368,228
Entities Providing Investment Services (Investment Companies)	22	23		597,032,743
The Central Depository	1	1		4,270,542
Credit Organizations	43	43		1,854,261,567
Investment Fund Managers and Entities Managing Non-Public Funds, including regarding Relations Related to the Management of Investment funds	79	80		3,070,657,766 (of which 2,604,711,396 under the management of pension funds
Entities Engaged in Foreign Currency Exchange	226	243[13]		5,038,827,974
Pawnshops	62	62		22,035,499
Insurance (Including Reinsurance) Companies	8	9		234,882,328
Entities Providing Intermediary Insurance (including Reinsurance) Services	4	4		1,054,330
Credit Bureaus	1	1		5,899,671

11. Imports from Iraq increased by 92% in 2021. In 2022, the same indicator decreased by 92%, and in 2023, it increased by 109%. Exports to Iraq increased by 8% in 2021 and 41% in 2022 but declined by 28% in 2023. The main exported products are tobacco and cattle. Imports from Syria rose by 97% in 2021 and 22% in 2022 but dropped by 55% in 2023. Exports followed a different pattern, with sharp declines of 65% in 2021 and 48% in 2022 before rebounding with an 83% increase in 2023. Imports from Lebanon grew by 4% in 2021, followed by a significant 124% increase in 2022, with the growth trend continuing in 2023. On the export side, trade from Armenia to Lebanon saw declines of 2% in 2021 and 10% in 2022. However, 2023 marked a strong recovery with a 123% increase.

12. Includes electronic money institutions and postal remittance.

** The company has appealed the decision of the CBA to revoke the license, the court case is in progress and CBA's decision has not entered into force yet.

13. This is the number of issued licenses to a total number of 177 firms.

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

A- Type of Entity - to be listed in descending order of size	B- Number operating	C- Provide services covered by the FATF standard	D – Explanation for order of listing	E- Total Annual Turnover (EUR[14])
Casinos (including organizers of games of chance and lotteries)	12	N/A	Based on the results of National/Sectorial risk assessments and market share (where applicable)	17,484,091,217
Real estate agents[15]	207	N/A		14,356,276
Advocates	2776	345		N/A
Sole Practitioner Lawyers and Legal Firms	1183	197[16]		606,817[17]
Notaries	121	121		N/A
Sole Practitioner Accountants and Accounting Firms	1077	253[18]		59,025[19]
Dealers in Precious Metals and Precious Stones	1024	N/A		303,203,052
Trust and Company Service Providers	N/A	N/A		N/A

27. The AT ranked sectors based on their relative importance in Armenia, their respective materiality and ML/TF risks. This approach was applied throughout the evaluation and was further used to weight positive and negative effectiveness issues aimed at informing conclusions and overall ratings.

28. Armenia's financial sector is strongly bank-dominated, with banks holding around 83% of total financial sector assets. Banks also have the broadest customer base and service range, and most are assessed as medium or high risk in the ML/TF NRA. The banking sector is the primary focus due to the nature of financial services and clientele, and the nature of control (ownership). About 58% of the banking system's statutory capital is held by foreign participants, with several banks forming part of larger international financial groups, which introduces additional complexity and cross-border risk considerations. Based on materiality and inherent exposure, the banking sector represents the most significant source of potential ML/TF risk in Armenia.

29. Over the past five years, Armenia's financial system has experienced substantial growth, in line with broader economic expansion, both in terms of assets and customer volumes, as well as in the number of operating institutions—particularly in the investment and securities sectors. The securities market in Armenia is developing, with bonds being the most traded instrument. Transactions are primarily carried out through financial institutions such as banks and investment companies, and there has been an increase in the trading of international securities. Investment firms were assessed as highly important due to their growing activity, particularly in brokerage of foreign securities and expanding cross-border operations.

30. Money value transfer services (MVTS) and electronic money institutions (EMI), while representing a small share of total financial sector assets, were also assessed as highly important due to their relevance for certain higher-risk activities. These services are mainly used for low-risk transactions

[14] The EUR exchange rate as of 31/12/2024: 413.89

[15] Number of deals per annum – 15 001; Value of deals per annum – 714,813,389 EUR; Number of Clients – 39 952

[16] While in 2024, 197 lawyers specified in their internal rules and procedures that they provide the services covered by FATF Standards, risk assessment analyses have indicated that in 2024 only 87 lawyers have conducted the services covered by the FATF standard.

[17] Turnover refers to the services provided in relation to the transactions covered by FATF standards.

[18] While in 2024, 253 accountants specified in their internal rules and procedures that they provide the services covered by FATF Standards, risk assessment analyses have indicated that in 2024 only 132 accountants have conducted the services covered by the FATF standard.

[19] Turnover refers to the services provided in relation to the transactions covered by FATF standards

like utility payments and face reduced risks due to strict measures such as linking electronic wallets to bank accounts or payment cards. However, despite these safeguards, risks persist in card-to-card transfers—especially via foreign payment systems—wallet-to-bank transactions, and cash deposits via ATMs, prompting further regulatory amendments.

31. Non-bank financial institutions generally present lower exposure due to structural constraints and were therefore assessed as moderately important. Credit organisations and pawnshops are limited to providing short-term loans, which must be cashless for amounts above EUR 48 as from 2024 (EUR 193 in 2022, EUR 121 in 2023), significantly reducing risks. Mandatory pension funds, which represent the second largest share of assets, face lower risks as participant funds are generated from state budget allocations and are primarily invested in low-risk instruments like publicly listed securities and bank deposits, with limited options for early withdrawal. Foreign currency exchange offices, while cash-intensive, constitute a low-materiality segment. These operations are restricted to cash transactions, with recent regulations requiring cash conversion to go through bank accounts.

32. Several financial sectors were assessed as having low or non-material exposure. The insurance sector remains low risk as Armenia currently has no life insurance market. Until early 2025, non-public investment funds and their managers operated outside the CBA's supervisory mandate and were only required to register fund rules. At the time of the onsite visit, no virtual-asset service providers (VASPs) had yet been licensed, as the regulatory regime under the 2025 Law on Crypto-assets was still being operationalised. This sector was therefore considered non-material for the assessment, with financial institutions required in the interim to treat crypto-related customers as high-risk and apply enhanced due diligence.

33. Within the DNFBP sector, online casinos and e-gaming platforms constitute by far the most material segment in Armenia, accounting for almost 99% of the gaming industry and generating the highest risk and transaction volumes. Accordingly, they were a primary focus of the AT. Real estate agents were also given particular attention and assessed as highly important, as property transfers are viewed by authorities as a prevalent money laundering method.

34. Other DNFBP sectors were assessed as moderately important, including notaries and advocates. Notaries in particular are considered among the higher-risk DNFBP activities due to their role in facilitating various transactions, though they remain smaller in scale compared to the gaming and real estate sectors.

35. Several DNFBP sectors were considered less material during the review period, in part due to the 2023 cashless legislation. This legislation effectively placed dealers in precious metals and stones and certain other cash-intensive activities outside the AML/CFT framework for most of the assessed period. The AT found no evidence of trust and company service provider activities despite indications in open sources, and this sector was therefore considered non-material for the assessment.

Legal persons and legal arrangements

36. Armenia permits the establishment of a broad range of legal persons and legal arrangements as summarized in the tables below.

Table 0.3. Legal Persons and legal arrangements - 31 December 2024

Type of legal person / arrangement – to be listed in descending order of significance	Total number registered
Limited Liability Company	100066
Public Organization	6907
Closed Joint-Stock Company	3156
Production Cooperative	2882
Foundation	1797
Condominium	797
Open Joint-Stock Company	725
Trade Union	702
General Partnership	567
Consumer Cooperatives	485
Agricultural Cooperatives	176
Political Party	123
Religious Organization	63
Employer's Union	35
Chamber of Commerce and Industry	12

Table 0.4. Numbers registered and terminated - legal persons and legal arrangements per year

Type of legal person/arrangement – to be listed in descending order of significance	2020 - Registered during year	2021 - Registered during year	2022 - Registered during year	2023 - Registered during year	2024 - Registered during year
Limited Liability Company	5700	6768	11723	10075	8381
Public Organization	336	522	426	427	445
Closed Joint-Stock Company	121	112	198	135	112
Production Cooperative	2	1	2	0	3
Foundation	121	145	132	104	104
Condominium	23	25	19	16	37
Open Joint-Stock Company	11	1	6	15	10
Trade Union	10	8	9	11	10
General Partnership	0	0	0	0	0
Consumer Cooperatives	7	9	8	2	3
Agricultural Cooperatives	22	13	25	15	22
Political Party	3	28	2	2	8
Religious Organization	3	1	1	4	0
Employer's Union	0	0	0	0	1
Chamber of Commerce and Industry	0	0	0	0	0

37. The most significant of these is the Limited Liability Company (LLC), which accounts for the majority of registered entities, with a total of 100 066 LLCs recorded as of December 2024. The Public Organizations, and Closed Joint-Stock Companies collectively account for a significant portion of legal persons in the country, with 6 907 Public Organizations and 3 156 Closed Joint-Stock Companies registered as of 2024. Legal entities such as Production Cooperatives, Foundations, and Trade Unions are also prominent, with 2 882 Production Cooperatives and 797 Foundations recorded by December 2024.

38. Condominiums, Open Joint-Stock Companies, Consumer Cooperatives, and other legal entities, including political parties and religious organizations, also contribute to the country's legal landscape, although their numbers are smaller.

39. Turning to the foreign ownership of Armenian legal persons, they account for about 15% of the overall population with the primary countries of origin of the owners/shareholders, and BOs from Russia, Iran, India, the UAE, the USA, and Georgia.[20] Authorities concluded that over 50% of the legal persons registered in Armenia with a foreign founder, manager or BO do not in practice conduct economic activity in the country and did not engage in transactions with reporting entities.

40. Armenia is not a signatory of Hague Convention. Armenian law does not permit establishment of trusts or other type of legal arrangements in Armenia.

Structural Elements

41. Since 2015, Armenia has introduced several measures to combat ML/FT, including revised Criminal Code and Criminal Procedure Code in 2021 that strengthened fight against corruption offenses and introduced criminal liability for legal entities. The ACC was established in 2021, followed by the creation of the Anti-Corruption Court and Appellate Court in 2022-2023. Legislative amendments between 2019 and 2023 enhanced integrity checks for key positions in the ACC, GPO, and courts. The declaration system was updated with new expense declaration mechanisms and an electronic submission system in 2023. Amendments to the Law on Public Service in 2022 improved conflict of interest and gift regulations.

42. Starting in 2024, heads of executive bodies of state and community non-profit organizations, state-established foundations, and commercial organizations with 50% or more state or community participation are required to submit situational declarations.

43. As of 2023, the requirement to declare beneficial owners was extended to all legal entities. Administrative and criminal liabilities were introduced for failure to comply with the declaration requirement, improper compliance, and submission of incomplete or false data. Simultaneously, an electronic platform for the register of beneficial owners of legal entities was launched.

Background and other Contextual Factors

44. Armenia’s economic environment demonstrates stable growth. Recovery from the coronavirus pandemic, coupled with the geopolitical situation, contributed to an increased inflow of capital and human resources into Armenia, driving economic growth. Additionally, efforts to reduce the shadow economy as a percentage of GDP have continued successfully, with a decline from 12–15% to 8.6%. Regarding free trade zones (FTZs), their location, participant numbers, and turnover volumes indicate that their operations do not pose significant ML/TF risks.

45. The population of Armenia remains largely homogeneous, with Armenians making up 98.06% of the population. There are no active terrorist groups in Armenia, and no nationals or residents appear on UN Security Council sanctions lists; and no terrorist financing cases have been identified.

46. Armenia has close trade relationships with Iran with whom the country shares borders. Authorities report that one Armenian bank conducts transactions with Iran (operations being conducted with a parent bank in Iran) to enable trade relations. Cross-border non-cash financial flows have remained broadly aligned with foreign trade turnover indicators.

47. A wide range of payment instruments is used in Armenia to meet the diverse transaction needs of individuals and businesses. Financial inclusion continues to show growth, reflected in the increasing number of users of financial services and the rising volume of non-cash transactions. Contributing

[20] 2024 NRA, par. 738.

factors include the opportunities provided by financial organizations, efforts to enhance financial literacy, and improved accessibility to financial services.

AML/CFT/CPF strategy

48. Armenia has developed four national strategies (2016–2018, 2019–2021, 2022–2024, and 2025–2028). The last three include an implementation action plan, and a monitoring tool.

49. The primary strategic goals are focused on the use of available resources to effectively fight evolving ML threats, prevent misuse of the financial system for ML/TF purposes, and enforce sanctions on offenders. To achieve these goals, the strategy prioritizes the understanding, assessment, and mitigation of ML/TF/PF risks; the effective investigation of ML cases; the risk-based supervision; the confiscation of criminal property; and the preventive measures.

50. Additionally, a communication concept and action plan for 2024–2026 was approved on 28 December 2023, as part of Armenia's broader Anti-Corruption Strategy. The strategy has five key objectives: preventing corruption, improving legal and institutional systems, enhancing public awareness, strengthening integrity in business, and improving monitoring and evaluation systems.

Legal & institutional framework

51. The Armenian Law on Combating Money Laundering and Terrorist Financing is the central element of legislation for AML/CFT/CPF matters. Other principal pieces of legislation include the Law on Confiscation of Property of Illicit Origin, the Criminal Code of Armenia, the Criminal Procedure Code of Armenia, the Law on Non-Cash Transactions, and the Law on Legal Assistance in Criminal Matters.

52. The institutional framework includes a large number of authorities, the most significant of which are the following.

53. The **Interagency Committee on Combating Money Laundering, Terrorism Financing and Financing of Proliferation of Weapons of Mass Destruction (Interagency Committee),** was established by decision of the Prime Minister of the Republic of Armenia No. 45-A from 17 January 2019. It acts as the high-level policy making and coordination body charged with AML/CFT responsibilities. The Interagency Committee convenes twice a year or whenever necessary to consider and make recommendations on issues related to national AML/CFT policy, cooperation of involved competent authorities, international and national developments and trends in the area.

54. The **Financial Monitoring Center of the Central Bank of Armenia (FMC)**, which is an administrative type FIU, is a structural unit of the CBA authorized to receive and request reports and other information from reporting entities and from state bodies; analyse information and disseminate/ exchange the results of its analysis, as appropriate; suspend suspicious transactions or business relationships; freeze the property of terrorism-related persons; develop, endorse and publish the lists of terrorism-related persons; supervise certain types of reporting entities for AML/CT compliance and apply responsibility measures; assist other supervisory authorities; develop by-laws and guidelines (including criteria and typologies of suspicious transactions) in the field of AML./CFT; give assignments with a view to ensure the reporting entities' proper implementation of their AML/CFT obligations; conclude agreements of cooperation with international structures and foreign financial intelligence bodies.

55. The **General Prosecutor's Office of Armenia (GPO)**: Prosecution authorities are designated to oversee and control the legitimacy of investigations into ML/FT cases, and to initiate and pursue prosecution against persons charged with such crimes in court. GPO is also responsible for handling

mutual legal assistance, as well extradition requests and requests for transfer of proceedings in the pre-trial stage.

56. The **National Security Service of Armenia (NSS)** is a national executive body in charge of formulating and implementing the RA Government’s policy in the field of national security, and administering the national security bodies. Within the AML/CFT framework the NSS is responsible for operational intelligence of ML and FT cases.

57. The **Investigative Committee of Armenia (IC)** is a national executive body in charge of investigating alleged crimes within its competence as defined under the CPC. Within the AML/CFT framework, the IC is responsible for investigation of predicate offences (other than corruption related crimes, which are mandated to the ACC).

58. The **Anti-Corruption Committee of Armenia (ACC)** as a body of inquiry under the CPC, is empowered to undertake preliminary and full pre-trial investigations into corruption-related crimes, including on ML proceedings, provided for in the CPC, where ML was committed through abuse of official authority, powers or related influence. In addition to its investigative mandate, the ACC is also responsible for conducting operational intelligence activities in support of its anti-corruption and ML functions.

59. The Police of the **Ministry of Internal Affairs of Armenia (MIA)** as a body of inquiry executing its powers stipulated under CPC and LOIA, which inter alia include undertaking the necessary operational-intelligence measures for detection of crime and forwarding the information to the investigator of the relevant law enforcement body with investigative powers (i.e. the IC, or the ACC).

60. The **State Revenue Committee of the Republic of Armenia (SRC)** is the principal government agency dealing with tax and customs matters. It executes its powers stipulated under CPC, which inter alia include undertaking the necessary operative-investigatory measures for detection of tax crimes. Since 2018 the SRC has served as the supervisory authority for casino operators, games of chance (including online gambling), and lotteries. In addition, NPOs in the RA fall under the oversight of the SRC.

61. The **Central Bank of the Republic of Armenia (CBA)** is authorized to license, register (some), regulate, and supervise all types of financial institutions and VASPs operating in Armenia. Sectorial laws regulating activities of various types of financial institutions and VASPs also provide for the CBA’s regulatory and supervisory function. Under the AML/CFT Law, the CBA is the authorized body verifying compliance of financial institutions and VASPs with AML/CFT requirements.

62. The **Ministry of Economy of Armenia (MOE)** is the Central Body for developing, implementing and assessing the results of the RA Governments economic policy. Within the AML/CFT framework, the MOE is designated as the authorized body in the sector of control over export of dual-use goods and provision of license/permits for their export.

63. The **Ministry of Finance of Armenia (MOF)** is a national executive body in charge of formulating and implementing the RA Government’s policy regarding the management of public funds, including tax and customs administration. Within the AML/CFT framework, the MOF is designated to license casino operators, games of chance (including online gambling), and lotteries.

64. The **Ministry of Justice of Armenia (MOJ)** is a national executive body in charge of formulating and systematizing/ coordinating Republic of Armenia legislation. In addition, it comprises separated divisions tasked with, inter alia, registration of legal entities, compulsory enforcement of judicial acts, and penitentiary functions. Within the AML/CT framework, MOJ is designated to: a) perform legal appraisal and state registration of secondary legislation; b) appoint and supervise the

notaries, and c) administer the State Register of Legal Entities. MOJ is also responsible for mutual legal assistance in trial stage.

65. The **Ministry of Foreign Affairs of Armenia (MOFA)** is a national executive body in charge of formulating and implementing the RA Government's policy in the area of foreign affairs. Within the AML/CFT framework, MOFA coordinates the process of conclusion and implementation of international treaties, accommodates membership of the country (and of its representative bodies) in international organizations, and regularly updates competent national authorities on the UNSC Resolutions in connection with TF and PF.

66. The **Judicial Department of Armenia (JD)** is a state administrative institution to provide for comprehensive and effective execution of the authorities vested in the courts and their participation in civil-legal relationships, through the General Assembly of Judges. Functions of the Judicial Department are set out in its Charter approved by the Chairman of the Supreme Judicial Council of the Republic of Armenia. Within the AML/CFT framework, the Judicial Department provides detailed statistics on ML/FT and predicate offence convictions.

67. The **Corruption Prevention Commission of Armenia** (**CPREVC)** was established as an autonomous state body in 2019, vested with institutional independence and a comprehensive mandate. The Commission is entrusted with a broad scope of powers, including: ensuring the integrity of persons holding public office; overseeing compliance with incompatibility requirements, conflict of interest regulations, other restrictions, and codes of conduct; regulating and managing the asset declaration system, including verification, analysis, publication, and maintenance of relevant registers; supervising the financing and annual reports of political parties; participating in the development, implementation, and monitoring of anti-corruption policies and corruption risk mitigation measures; and designing and implementing integrity-building and anti-corruption education and awareness programs.

68. The **Chamber of Auditors and Expert Accountants of Armenia** (**Chamber of Auditors)** is an SRB and is the sole accredited body overseeing its member audit organizations. Additionally, the supervisory authority participates in the external assessment working group and directly conducts external assessments. Its activities are inspected by the Public Oversight Council for Accounting and Audit Activities (AAPOC) under the MOF.

69. The **Chamber of Advocates of Armenia** (**ChoA)** is an SRO responsible for qualification and licensing of advocates. Activities of the Chamber of Advocates are regulated by the Advocacy Law. The Chamber of Advocates also supervises activities of licensed advocates in terms of AML/CFT.

Preventive measures

70. Preventative measures are set out in the AML/CFT Law and secondary legislation and are broadly compliant with the FATF Standards. FMC and Supervisory authorities have issued additional guidance documents and assignments to assist FIs and DNFBPs with an implementation of AML/CFT requirements.

71. DPMS do not fall under the FATF standard due to the established cash transaction threshold, which prohibits transactions above EUR 700 from being paid in cash- a threshold below the EUR 15 000 defined by FATF for DPMS regulation. Other entities that do not fall under the FATF standard, however, Armenia has chosen to subject them to AML/CFT/TFS regulation are pawnshops and auditing firms (see Table 0.5 below).

Supervisory arrangements

72. Financial institutions and VASPs are supervised by the CBA. VASPs became subject to AML/CFT/TFS regulation recently, in August 2025. DNFBPs are supervised by several competent authorities and/or SRBs: casinos – by the SRC; notaries – by the MoJ; advocates – by the ChoA; real estate agents, legal professionals other than advocates, accountants are supervised by the FMC.

Table 0.5. Supervision of FI, VASP and DNFBP sectors – 31 December 2024

Type of Entity	Name of agency responsible for registration/ licensing	Name of general supervisor	Name of AML/CFT supervisor	Name of TFS supervisor
Banks	CBA	CBA	Banking Prudential Supervision Service of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Entities Engaged in Money (currency) Transfer Services[21]	CBA	CBA	Payment System Participants Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Entities Providing Investment Services (Investment Companies)	CBA	CBA	Market Conduct and Securities Market Participants Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
The Central Depositary	CBA	CBA	Market Conduct and Securities Market Participants Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Credit Organizations	CBA	CBA	Microfinance Organizations Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Investment Fund Managers and Entities Managing Non-Public Funds, including regarding Relations Related to the Management of Investment funds	CBA	CBA	Market Conduct and Securities Market Participants Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Entities Engaged in Foreign Currency Exchange	CBA	CBA	Microfinance Organizations Supervision of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Pawnshops	CBA	CBA	Microfinance Organizations Supervision of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Insurance (Including Reinsurance) Companies	CBA	CBA	Insurance Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Entities Providing Intermediary Insurance (including Reinsurance) Services	CBA	CBA	Insurance Supervision Division of the FSLD of the CBA; AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
VASPs	CBA	CBA	Market Conduct and Securities Market Participants Supervision Division of the FSLD of the CBA AML/CFT and Sanctions Compliance Risk Assessment Division of the FSLD of the CBA	
Casinos (including organizers of games of chance and lotteries)	MOF	SRC	Division of Oversight of the Activities Games of Chance, Casinos and Lotteries of the SRC	

[21]. Includes electronic money institutions and postal remittance.

Real estate agents	N/A	FMC	Strategic Analysis and Supervision Division of the FMC
Advocates	Chamber of Advocates	Chamber of Advocates	Chamber of Advocates
Sole Practitioner Lawyers and Legal Firms	N/A	FMC	Strategic Analysis and Supervision Division of the FMC
Notaries	MOJ	MOJ	Control Department of the MOJ
Sole Practitioner Accountants and Accounting Firms	N/A	FMC	Strategic Analysis and Supervision Division of the FMC
Auditors and Audit Firms	N/A	Chamber of Auditors	Chamber of Auditors and Expert Accountants
Dealers in Precious Metals and Precious Stones	N/A	FMC	Strategic Analysis and Supervision Division of the FMC
Auction Organizers	N/A	FMC	Strategic Analysis and Supervision Division of the FMC

International co-operation

73. Armenia has a legal framework in place for international co-operation. The international co-operation requests for mutual legal assistance and extradition are handled by two authorities depending on the state of criminal proceedings: i) the GPO is responsible for providing legal assistance, including procedural actions and extradition requests, in criminal cases under pre-trial proceedings and ii) the MOJ is responsible for legal assistance in cases under court proceedings, including the execution of judgments. The FMC engages in international co-operation both through membership in international organisations and bilateral relations. The CBA, a financial supervisor, is authorised to co-operate with foreign financial supervision bodies in the framework of bilateral and multilateral agreements.

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

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

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Since the 2015 Mutual Evaluation Report (MER), Armenia has conducted three National Risk Assessments (NRAs) to understand the money laundering (ML) and terrorism financing (TF) risk exposure: the 2017 NRA, the 2021 NRA, and the 2024 NRA. The 2024 NRA is based on a methodology developed by the Armenian authorities and covers data from 2021 to 2023. The authorities' understanding of risk is entirely based on the findings of the NRAs.

b) The main ML threats identified in the 2024 NRA stem from fraud, embezzlement, corruption, tax crimes, drug trafficking, and cybercrime. Compared to the 2015 MER findings, which indicated a lack of consensus among Armenian authorities regarding the most prevalent criminal activities for ML, now the perception is more unified. The ML residual risk level remained the same across all three iterations of the NRA.

c) The authorities' risk understanding of domestic versus foreign ML threats is an area for improvement as the 2024 NRA does not distinguish between the two. Even where foreign threats are acknowledged by the authorities, they are not specified and understood in depth, creating a situation where there is the perception that Armenia is disconnected from external threats. The 2024 NRA presents a limited analysis of the formal and informal incoming international requests especially by predicate offences and relevant typologies.

d) TF threat level is assessed as low based on the absence of cases and ongoing monitoring of financial flows. The list of high-risk countries is shared with the reporting entities. All those are positive outcomes. However, no analysis on the possible TF connections with organised crime is presented in the 2024 NRA. TF controls and TF risk exposure by FIs and DNFBPs by product and services has not been separately assessed, limiting authorities' and reporting entities' TF risk understanding and the ability to adopt mitigating measures that target specifically TF.

e) ML and TF risks in relation to virtual assets (VAs) were assessed to a certain extent. Authorities reported that TF risks in relation to virtual assets are low. Given that the virtual asset service providers (VASPs) sector was not regulated at the time of the on-site, while VASPs were operating in Armenia, it appears that there are insufficient elements to reasonably substantiate a low risk of abuse from VAs.

f) At the policy making level, authorities are guided by the National Strategy on AML/CFT (2025-2028) and the Anti-Corruption Strategy (2023-2026). The implementation of the National AML/CFT Strategy and the action plan are being monitored semi-annually.

Actions pertaining to supervisory authorities are not linked to higher materiality and risk areas, except for VAs.

g) The Interagency Committee serves as the authorized body responsible for national policy development and coordination of activities in the field of AML/CFT. The Committee proved to have valuable input when it comes to strategic coordination. Operational cooperation and coordination between competent authorities is not systemic and needs to be further strengthened.

Key Recommended Actions (KRA)

a) Armenian authorities should take action to deepen the national ML risk understanding by including other sources of information such as the incoming international requests (formal and informal) by predicate offence, and typologies of cross-border and organized crime concerning relevant predicate offences such as drug trafficking. The authorities should re-examine the impact of the foreign ML threats and the overall impact on the overhaul ML risk of Armenia. Proportionate mitigating measures should be taken at a national level.

b) Authorities should distinguish between ML and TF threats, vulnerabilities, and residual risks for FIs and DNFBPs by products and services. For VAs, a more comprehensive analysis of potential TF risk of abuse is needed (for example, using international reports, estimating the activity of VASPs on the national territory, estimating the VAs turnover, sectors where VAs are particularly used, etc.). Proportionate mitigating measures at a national level should be subsequently taken.

Other Recommended Actions

a) Authorities should enhance the TF risk analysis by (i) analysing the TF threats originating from illegitimate activities, such as organised crime or drug trafficking, and TF vulnerabilities from informal remittance services or any other unlicensed activity. TF-specific action points should be added in the national policies and strategic documents.

b) The authorities should also re-examine the materiality and risk related to real estates, including the relevance of the threshold envisaged for the obligation to notarise the transactions. The implementation of the resulting mitigating measures should be prioritised.

c) Armenia should ensure that in AML/CFT strategies, actions pertaining to supervisory authorities cover all higher materiality and risk areas.

d) Armenian authorities are to engage in more regulation and guidance on what constitutes a ‘low risk’ for simplified due diligence purposes, for example, what is implied by effective and sufficient AML/CFT supervision to categorise financial institutions as low risk, and in relation to government bodies that are domiciled abroad.

e) Armenia should enhance the existing operational cooperation mechanisms, through integrated platforms to ensure that cases are jointly initiated, merged, or developed, where all the possible sources of information are exploited and synergies created.

Overall conclusion on IO.1

Armenia has made commendable efforts following the 2015 MER and has demonstrated a clear political commitment to acquire a good ML and TF risk understanding, in particular in relation to corruption. ML risk understanding pertaining to the foreign threat and the associated predicate offences needs to be re-examined, since it is not specified and understood in depth. The risks related to the real estate sector are acknowledged when related to predicates such as corruption and fraud, but more analysis is needed on the materiality (legal persons vs natural persons) and on the effect of the planned mitigating measures. Authorities carry out regular monitoring of financial flows for ML and TF risks. The authorities concluded that the threat level related to TF is low but further enhancement is needed to ascertain the reasonableness of the rating. The national policies and strategies to address the ML and TF risks are generally adequate. The implementation of the National AML/CFT/CPF Strategy for 2025 to 2028 and the action plan are being monitored semi-annually, where the progress on implementation is discussed within the Interagency Committee. Some authorities showed how their own objectives and activities are largely consistent with the ML/TF risks identified in the 2024 NRA and with the actions envisaged in the AML/CTF National Strategy. National cooperation and coordination take the form of a case-by-case basis.

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

1. Since the last evaluation round, Armenia has completed three NRAs: in 2017 based on data for the period 2014-2016 (2017 NRA), in 2021 based on data for the period of 2017-2020 (2021 NRA) and the 2024 NRA based on data covering 2021 to 2023. This last iteration of the NRA is based on a methodology developed by the Armenian authorities and includes an improved analysis of a broad range of risks that the country is facing with the highest focus on the vulnerabilities. However, some concerns are expressed that impact the overall ML risk understanding and mitigation efforts by the country as evidenced below.

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

1.1.1. ML risks

2. Armenia has to be commended for actively engaging in efforts to continuously improve the understanding of the landscape of risks, by conducting three NRAs since the last evaluation round. The country does not record any significant change in the ML risk landscape since the 2015 MER, which, seeing the global developments in the ML/TF risk environment in the last ten years, constitutes an area for concern.

3. The authorities' understanding of risk is based on the NRA and is to some extent considered as generally good, with some areas for improvement. The strategic analyses carried out following the NRA (presented under core issue 1.2) are all driven from findings from the NRA, and in discussions during the on-site with both the law enforcement and the supervisory authorities, as well as with the reporting entities, the main focal point of risk understanding was always the NRA.

4. The most recent NRA was finalised in 2024 and conducted by a working group established under the auspices of the Interagency Committee, which included representatives from the law enforcement,

supervisory authorities, representatives from key Ministries[22] as well as engagement of the private sector representatives.

5. The main ML threats identified stem from fraud, embezzlement, corruption, tax crimes, drug trafficking, and cybercrime.[23] The AT considers this conclusion as reasonable, especially when speaking about the domestic threat.

6. Based on the provided statistics and on-site discussions, the fraud category in most cases overlaps with embezzlement and cybercrime, therefore, for clarity and consistency throughout the report, these ML threats will be referred to as "fraud". Compared to the 2015 MER findings, which indicated a lack of consensus among Armenian authorities regarding the most prevalent criminal activities for ML[24], for the period under review, the perception on the main ML threats is now more unified.

7. A development from the previous MER is that the authorities have included an estimation of the magnitude and significance of the overall proceeds from criminal activity. Nevertheless, the estimation includes only reported crime and does not extend to unreported crime. A separate document was provided on the extent of unreported crime, which does not seem to have impacted the ML/TF threat level in the 2024 NRA. The analysis in the 2024 NRA does not look at incoming international co-operation requests by predicate offence, given that this data started being collected in 2023.

8. The AT notes that according to the NRA, there has been no change in the threat level despite global dynamics in the ML/TF risk landscape in the last ten years, and the economic and demographic developments in Armenia post 2022. Although the CBA demonstrated a better understanding of those changes, some concerns remain, mostly linked to the level and features of the external threat. The general conclusion of the 2024 NRA is that the "cross-border" predicate offences do not significantly impact the country's ML/TF risk profile[25], a view which was mirrored in general by the authorities' understanding, who consider the ML threats to be almost exclusively local.

9. Nevertheless, the AT notes that according to the NRA, 59%[26] of the funds involved in ML STRs have a foreign nexus. The authorities maintain that some of these represent funds generated domestically, sent abroad and then returned, while others constitute proceeds from foreign predicates. There is no breakdown on the proportion of each of these two categories, nor on the underlying criminality. Recent and trending large-scale fraud cases linked to the so called "call centres" established in Armenia with foreign funds were noted, where the predicate offences (fraud) are committed in Armenia with the proceeds being laundered abroad (the authorities have not detected related returning funds). While accepting authorities' explanation as reasonable, the AT considers that the foreign threat should be further explored by the analysis of recent trends, cases, their typologies, and international sources.

10. The AT also notes that the 2024 NRA found that the total number of customers of banks has shown an increasing trend, reaching an average growth of 4.25% against 1.5% in the 2021 NRA, an increase attributable to the non-resident natural persons. Additionally, findings in international reports[27] present that in 2024, 28% of the assets held by commercial banks were of foreign ownership. These two

[22] This included representatives from the prosecutors' office, the anti-corruption committee, the National Security Services, the Investigative Committee, the Ministry for Internal Affairs, the State Revenue Committee (SRC), the Ministry of Justice, the Ministry of Finance, the Ministry of Foreign Affairs, Ministry of Economy, the Judicial Department, Chamber of Advocates, Chamber of Auditors, Chamber of Auditors and Expert Accountants, and the Central Bank.as well as engagement of the private sector representatives.
[23] 2024 NRA, para. 185-186.
[24] 2015 MER, para. 94.
[25] 2024 NRA. page 10.
[26] The authorities explained that this conclusion was drawn on the basis of the entire population of STRs and not limited to those that triggered a dissemination to LEAs. Speaking of the latter, only 20% of the STRs would include a foreign nexus.
[27] Global forum on transparency and exchange of information for tax purposes, peer review report on the exchange of information on request – Armenia, 2025 (second round, combined review), p. 29, par. 39.

findings, albeit not presenting anything suspicious on their own, indicate however that the foreign involvement is increasing.

11. Armenian authorities uniformly reported that the threat emerging from transnational organised criminal networks dealing in drug trafficking and other major crimes is negligent. Most LEAs consider the threat of organized crime to be low, describing offences (mainly fraud and drug-trafficking) as small-scale and domestic in nature. The authorities acknowledge the existence of large-scale drug trafficking cases, which have been considered for the NRA purposes, but remain of the view that this does not constitute a trend and typology in the country.

12. The AT has concerns about the reasonableness of this conclusion, and is of the view that the risk assessment should explore more the impact of the criminal activities carried out by transnational organised criminal groups (e.g. drugs), particularly in the context of increasing smuggling and illegal trade of non-renewable resources, such as gold and diamonds, involving both domestic and foreign organised criminal groups, and reports indicating Armenia as being used as a transit country for illicit drugs.[28]

13. Authorities assess ML/TF vulnerabilities of the legal, and the institutional systems taking into consideration the particularities of the FIU, LEAs, the judicial system, the supervisory bodies (FIs and DNFBPs), data reliability and usability, international cooperation, domestic cooperation, confiscation, and additional preventive measures to fight terrorism and TF. Higher ML/TF vulnerabilities are found in LEAs specifically in relation to the need for increased human and technical resources; the judiciary, in view of the delays in ML trials and absence of specialised courts; and the limited supervision in the gaming sector, notaries, and advocates. Although the AT is not challenging these conclusions, it is not clear how some of the conclusions were reached. For example, on the vulnerabilities of the preventive measures to combat terrorism and TF, no analysis is presented on what are mitigating measures by type of product and service, and how are these leading to a lower vulnerability. Additionally, in the assessment of the sectoral legislation, reference is made to legislative initiatives that are not yet in place, for example, in relation to the transparency of legal persons[29].

14. Authorities also assessed ML/TF vulnerabilities of the financial institutions and the non-financial reporting entities, the legal persons and the non-profit organisations (NPOs). In the financial sector, the ML/TF vulnerabilities were rated as 'medium' (score 2 out of 4), with the main vulnerability lying in the product/service risk due to VAs, specifically due to the annual turnover in the sector[30] which authorities reported as difficult to assess especially in relation to the nine to ten VAs ATMs present in the country[31].

15. In the non-financial sector, the highest vulnerability for ML/TF were detected to be in the gambling and the real estate sectors, namely because, in both sectors, between 2021 to 2023 the inspections and enforcement action taken were very low. The authorities see the risks related to the real estate transactions often linked to proceeds from corruption and fraud. In terms of ownership of real estate, natural persons outweigh legal persons, which however hold higher-end properties. Data collected by authorities shows that between 2021 to 2024, natural persons acquired 96% of the real estate vs 4% for legal persons. However, the average value of a legal person real estate contract is

[28] Global Organised Crime Index, Report on Armenia, 2025, page 3, and United States Department of State Bureau of International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report, Volume 1, March 2022, p. 81 https://www.state.gov/wp-content/uploads/2022/03/22-00767-INCSR-2022-Vol-1.pdf

[29] 2024 NRA, par. 751-753

[30] About EUR 182 million to EUR 193 million

[31] 2024 NRA, par. 662.

between 2,4 to 7 times higher than the average for a natural person[32]. It is not clear how this materiality aspect was reflected in the 2024 NRA or in the risk understanding by the authorities.

16. At the time of the on-site visit real estate transactions did not require the mandatory involvement of a notary. For the 2024 NRA, the authorities analysed the STRs and noted that the real estate associated amounts exceeded EUR 110 000. Aware of this vulnerability, the authorities made sure that the AML/CFT Strategy includes legislative amendments to introduce the obligation to notarise the real estate transactions above EUR 110 000, thus ensuring the implementation of CDD and the submission of STRs by this category of reporting entities. Although the authorities are to be commended for this relevant finding, this recommendation was not yet in place by the time of the on-site visit. The AT encourages the authorities to deepen the vulnerability analysis of the real estate sector to make sure it sufficiently encompassing the specific risks and laundering typologies.

17. Use of cash was identified as a vulnerability which the authorities addressed through a law on non-cash transactions, effective as from July 2022, and mandating non-cash payments for most of the transactions over approximately Eur700. No information was provided on the results of this mitigating measure (such as increased number of TTRs or STRs or others – see also IO5).

18. The risk understanding of the supervisory authority of the financial sector appears to be more developed than that of the supervisory authorities of the non-financial sector, especially with regards to ML typologies specific for their sectors.

19. On ML/TF vulnerabilities related to legal persons, authorities report that LLCs are the most material and considered to be more vulnerable in view of the organizational and legal form, and the ease of incorporation.[33] LLCs in Armenia increased from 6,768 new registrations in 2021 to 10,075 new registrations in 2023. Vulnerabilities in relation to all types of legal persons were found to be (i) the non-dissuasive penalty for failure to retain the accounting documents of a legal person, enabling criminals to dissimulate their traces, creating challenges for LEAs in gathering evidence; (ii) the challenge in identifying BOs of non-resident legal persons, and (iii) the absence of the necessary mechanisms for the effective operation of the BO disclosure system. Authorities conclude that the ML/TF vulnerabilities of legal persons are medium. While the identified vulnerabilities are reasonable, the AT has some reservations on the overall risk level, as explained under IO.5.

20. The 2024 NRA notes that vulnerabilities arising from VAs remain high, due to difficulties in assessing the entire volume of transactions related to VAs in Armenia[34] (materiality) as well as the absence of regulatory (supervisory) measures. The authorities acknowledge the main respective threats to be deriving from drug and fraud proceeds. Following the 2024 NRA, a strategic analysis of ML/TF/PF risks associated with VAs transactions was conducted in 2025 as well as a typology study in relation to the use of VAs in drug trafficking.

1.1.2. TF risks

21. TF risk was considered in all the iterations of the NRA. During the on-site, Armenia reported that there is a separate TF risk assessment besides the section in the 2024 NRA, however the document was not made available to the AT due to high confidentiality nature of the data.

22. TF threats are considered through the prism of conflicts driven by religious or ethnic movements, minority rights violations, extremist propaganda, the presence of terrorist organisations, instances of terrorism and TF, and connections with high-risk countries.

---

[32] In 2023 natural persons totalled 47,770 contracts with an average contract value of circa EUR 40 300, and legal persons totalled 2,362 contracts with an average contract value of circa EUR 283 700

[33] 2024 NRA, par. 767.

[34] 2024 NRA, par. 662.

23. The authorities concluded that the threat level related to TF is low, given that: (i) there were no favourable preconditions for terrorism and TF in Armenia, (ii) competent authorities effectively prevented attempts by individuals associated with terrorist organisations, (iii) criminal proceedings were initiated in four cases related to terrorism and the preparation of terrorism, which are not significant in terms of TF, (iv) Armenia's relations with high-risk countries that include money transfers, are limited to the natural ties it maintains with Armenian communities, and (v) no significant risks related to terrorism were identified and the hypothesis put forward regarding TF have been refuted.[35]

24. Authorities have developed a list of TF high-risk jurisdictions that is regularly revised based on various factors such as: the FATF list of high-risk jurisdictions, international indices, and intelligence data from the FMC and the NSS. This list is communicated to the financial institutions, and comprehensive data on these high-risk jurisdictions is collected regularly by the FMC every six months. Authorities reported that there were no new findings or new trends from the financial flows analysis.

25. The assessment of Armenia's connections with high-risk countries included as well: i) individuals that moved to Armenia[36], ii) the preventive measures taken by banks when opening bank accounts in Armenia to citizens of high-risk countries, and iii) the vulnerabilities of NPOs registering and operating in Armenia from the perspective of TF. Authorities reported that no data was received regarding any TF cases involving NPOs registered and operating in Armenia, thereby concluding that NPOs have a low TF vulnerability.

26. Authorities reported that a strategic analysis was carried out in 2025 on the TF risks of VAs which was considered to be low. However, this needs to be developed further in the next NRA by taking into consideration all the sectors that involve the use of VAs and distinguishing clearly for all the sectors between ML and TF risks. The AT notes that VAs are an emerging risk globally, while the VASPs sector in Armenia was not yet regulated at the time of the on-site.

27. The authorities looked at the 1 713 cash declarations between 2022 and 2023, (almost five times higher than the figures recorded in the 2017-2020 NRA), and saw no TF suspicions.

28. Authorities' and reporting entities' TF risk understanding mirrors the 2024 NRA, since they view TF risks as low because there were no TF cases in Armenia.

29. Turning to legal persons, authorities' understanding is that the vulnerability is low on the basis of lack of TF cases (including criminal procedures) involving legal persons, their shareholders and BOs, and absence of international co-operation requests.

30. The AT notes that the authorities, specifically the financial supervisory authorities, have a good understanding of TF risks. Some areas for improvement that could lead to a better TF risk understanding include:

a) Further analysis to ascertain the reasonableness of a low TF risk of abuse through VAs.

b) An analysis on how TF threats take into consideration the origins of terrorist funding from illegitimate activities, such as organised crime, drug trafficking or similar, as well as the analysis of informal remittance services or any other unlicensed activity (see more in IO.9).

c) More analysis on the threats, vulnerabilities, and effectiveness of mitigating measures regarding legal persons.

d) TF controls and TF risk exposure by FIs and DNFBPs by product and services.

[35] 2024 NRA, par. 236.
[36] Mostly ethnic Armenians citizens of Syria and Lebanon.

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

1.2.1. Policies and activities to address ML risks

31. To address national ML/TF risks Armenian authorities developed: i) the National AML/CFT/CPF strategy (2022 to 2024) and a subsequent National AML/CFT/CPF Strategy (2025 to 2028), as well as a National Anti-Corruption Strategy for 2023 to 2026. Additionally, based on the outcomes of the NRA, the FMC carried out and completed 25 strategic analyses, in relation to a broad range of relevant topics such as significant international financial flows countries, possible TF-risky transactions (Regional level operation), banks and their non-resident customers; the internal monitoring of the reporting entities, etc.[37] These analyses, are being used by the reporting entities, by the law enforcement and the supervisory authorities. For example, the strategic analysis on laundering of funds obtained as a result of fraud was used by the reporting entities who revised their internal legal acts and strengthened onboarding and ongoing due diligence, LEAs used disseminations from the FMC as well as the typology in general to initiate or uncover criminal cases involving ML and/or fraud, and the supervisory authorities took the typologies identified into their inspection plans.

32. The 2022-2024 Strategy had three intermediate outcomes: i) understanding and mitigation of ML/TF/PF risks through domestic coordination of policies and international cooperation, prevention, ii) detection and reporting of proceeds of crime and funds in support of terrorism, and iii) detection and disruption of ML/TF threats where criminals are sanctioned and proceeds of crime and terrorist resources are confiscated. These outcomes included 75 actions, of which 36 were operational, 11 legislative, 5 institutional and 23 supportive.

33. Implementation of strategic goals largely focused on increasing resources (staff, knowledge and expertise) in law enforcement and investigative authorities, as well as increasing the understanding of ML/TF risks, strengthening AML/CFT supervision especially of the financial sector followed by assistance to the reporting entities to better implement AML/CFT measures. All the strategic goals were drawn on the basis of the identified vulnerabilities.

34. Authorities report that technically all actions linked to the 2022-2024 National Strategy have been addressed, except five. The unaddressed actions were followed up and included into the National AML/CFT/CPF Strategy for 2025-2028 together with other actions. One of these five action points that is still unaddressed, for example, calls for improving resources available in the LEAs for conducting parallel financial investigations.

35. The 2025-2028 Strategy has five strategic priorities: i) understanding, assessment and mitigation of ML/TF/PF risks; ii) effective investigation of ML cases; iii) risk-based supervision; iv) execution of confiscation; and v) preventative measures. These strategic actions, similar to the previous strategy, broadly cover the AML spectrum. There are in all 18 strategic tasks with 67 actions, of which 34 actions are operational, 6 legislative, 2 institutional, and 25 supportive. The strategic action plan of the current strategy is being monitored semi-annually, through qualitative and quantitative assessment criteria.

36. All of the above actions are aligned with the ML risks, and are measurable, constituting important elements for improving AML/CFT landscape.

[37] Strategic analysis carried out included: the ML/ preventive measures for cash transactions; three analysis on virtual assets that focused on the financial institutions' performance of obligations related to money transfers, their involvement in virtual assets, and the laundering of proceeds of drug trafficking through the use of virtual assets; ML/TF vulnerabilities of legal persons; card fraud cases, and the call-centre schemes; cash-based currency exchange transactions; on money mules and the detection of suspected money mules in the banking system; on cross border transportation of cash; analysis of ML/TF risks linked to transactions in the gambling sector, and in the real estate transactions, and customers of payment institutions.

37. Authorities reported that priority in the actions is shown by the deadline. The AT noted that some of the actions with a deadline set as December 2025 and therefore of higher priority relate to legal persons which in the 2024 NRA have a medium ML residual risk.

38. The AT also notes that the qualitative and quantitative assessment criteria are rather general and not always linked to measurable outcomes. For example, when making reference to 'high-quality requests' in relation to MLAs, criteria need to be presented on what constitutes high-quality.

39. With regards to the Anti-Corruption Strategy for 2023-2026, Armenia is to be commended for its the political commitment and infrastructure development to fight this crime, in line with the AML/CFT risk assessment. This strategy has five goals: preventing corruption and strengthening integrity systems with 26 actions, improving legal and institutional systems for combating corruption with 21 actions, anti-corruption education and improving public awareness mechanisms with 15 actions, business integrity, protecting business rights and facilitating state-business administration with 15 actions, and enhancing anti-corruption monitoring and evaluation system with six actions.

40. The Anti-Corruption Strategy could use more clarity on how the action plan should be prioritised. For example, prioritise actions that involve large-scale corruption and allocate resources accordingly.

1.2.2. Policies and activities to address TF Risks

41. In the 2025-2028 AML/CFT Strategy, the majority of the strategic actions are presented as addressing jointly ML/TF. There are few action points directly targeting TF aspects, which are mainly the sub-actions of general ML/TF related actions[38]. The limited action points directly targeting TF mirror the lower residual risk in the 2024 NRA.

42. Similar to the policies and activities to address ML, the strategic action plan on the TF action points is being monitored semi-annually, through qualitative and quantitative assessment criteria. Given the improvements needed of the TF risk assessment and risk understanding explored in the previous section, more TF action points should be introduced.

1.3. Exemptions, enhanced and simplified ML/TF measures

43. Currently, there are no exemptions from the AML/CFT framework. SDD is applied in low risk scenarios, where reporting entities may take lighter measures for ongoing due diligence of the business relationship in the following cases: FIs, government bodies, local self-government bodies, state non-commercial organisations, community administrative institutions, life insurance policies below a certain threshold, insurance policies for pension schemes, payments relating to salaries, allowances, utility services, pensions, also payments to the state authorities. These scenarios appear to be reasonable and are not contradicted by the NRA, with the two caveats below.

44. Authorities maintained that FIs would fall under the category of 'low risk' only in cases when they have effective AML/CFT supervision, without this being spelled out in a legal or regulatory document. The reporting entities itself should satisfy themselves that supervision is "sufficient" as no further guidance is provided in this respect. Although the authorities reported that this is rarely used in practice, the AT considers that more regulation and guidance is needed on this front.

45. With regards to the government bodies, additional guidance and clarification would be needed on those domiciled abroad.

[38] These are: conducting parallel financial investigation when there are investigations of terrorist-related alerts or cases to identify or disclose TF cases; incorporating the technical guidance on investigations of TF offences in the training programs for LEAs, and one action with three sub-action points on NPOs.

46. Enhanced due diligence (EDD) is applicable for certain higher risk situations and customers, both at onboarding stage and in the course of the business relationship, where such higher risk situations are politically exposed persons (PEPs), customers domiciled in FATF high-risk jurisdictions and countries identified as high risk for TF purposes, clients with complex or unusual large transactions or unusual transactions or business relationship with no apparent economic or other lawful purpose, private banking business, clients with non-face to face transactions or business relationships, legal persons or legal arrangements that are personal asset-holding vehicles, companies that have nominee shareholders or shares in bearer form, cash-intensive businesses and complex corporate structures. Correspondent banking relationships require additional measures under a different preventive regime. Although not all high-risk scenarios (for example legal persons or legal arrangements) are directly derived from the NRA results, the other enhanced measures directly target corruption or the highest national risks in Armenia such as the use of cash.

47. Some NRA driven higher risk criteria were included in the Guidance on Criteria on Suspicious Activities, as well as in the Guidance on Typologies (e.g. on VAs). Though these Guidelines do not require the application of EDD, any match with the criterion or typology requires consideration on reporting an STR supported with a comprehensive analysis, similar to EDD.

1.4. Objectives and activities of competent authorities and SRBs

48. According to the authorities, the national strategies are binding structural requirements with a clear deadline and identified responsible agencies for the integration of the national policy into internal work plans, where all relevant bodies (CBA, SRC, GPO, IC, ACC, NSS, MIA, MOJ, FMC) must provide annual programs of activities or relevant acts (a decision, order, recommendation, etc.) addressing the actions stipulated in this Strategy by June 2025.

49. As a result of the national strategies, in the period under review, the CBA strengthened its AML/CFT supervision, through various actions, such as the approval of the risk assessment methodologies for ML/TF/PF applicable to banks and non-bank financial institutions, or legal developments on VAs. New reporting templates were developed to enhance statistical monitoring of property confiscations based on court decisions. Resources at CBA remained stable throughout the assessment period and are considered adequate by the AT in relation to the size of the financial sector. An increase of about 50% is projected by end of 2027, reflecting expanded supervisory responsibilities, including the recently approved licensing and supervision of VASPs. (see IO.3)

50. Based on the findings of the 2024 NRA, the FMC took steps to strengthen the use and effectiveness of information provided to LEAs. This included an assessment of the outcomes resulting from the use of FMC data, as well as LEAs' evaluations regarding the quality of the information received. The findings have been submitted to the Office of the Prime Minister. FMC took the first steps to oversee compliance by some DNFBPs. All these are positive developments.

51. LEAs report that three positions have been allocated within the anti-corruption committee for financial investigators. As of 1 January 2023, the Investigative Division of the SRC and, as of 1 January 2024, the Investigative Department of the NSS ceased their operations within these respective bodies and were fully transferred, along with their positions and functions, to the IC. The NSS and SRC have not provided any additional information regarding the involvement of individuals for the implementation of the financial investigation function.

52. Some authorities, for example, the CBA and the IC have explained how their own objectives and activities are largely consistent with the ML/TF risks identified in the 2024 NRA and with the actions envisaged in the AML/CTF National Strategy. Other authorities' (GPO) objectives and activities were less aligned.

53. The issue of insufficient human resources in LEAs, although important, was unaddressed in the 2022-2024 AML/CFT Strategy, and was included as an action item in the 2025-2028 AML/CFT Strategy.

54. For the first time, the 2025-2028 AML/CFT Strategy has designated SRBs as responsible parties for strategic actions aimed at enhancing the supervision of the DNFBPs under their oversight.

55. To reduce vulnerabilities related to the judiciary, as identified in the 2024 NRA, the nomination of the Supreme Judicial Council as a member to the Interagency Committee was confirmed on 27 December 2024. Moreover, the 2025-2028 AML/CFT Strategy outlines actions for the Supreme Judicial Council to adopt appropriate approaches aimed at reducing the time limits for ML proceedings pending trial. Little progress has been achieved on this front before the on-site visit.

56. The AT notes that the 2025-2028 AML/CFT Strategy makes reference to the higher risk predicates that are in line with the 2024 NRA only for actions that fall under the remit of LEAs. Actions pertaining to supervisory authorities are not linked to higher materiality and risk areas, except for VAs.

1.5. National co-ordination and cooperation to develop and implement policy

57. In Armenia, the Interagency Committee acts as the high-level policy making and coordination body charged with AML/CFT responsibilities. The committee is composed of 18 senior representatives of all relevant stakeholders, except for some SRBs (for example the Chamber of Advocates). Since the 2015 MER, the Deputy Minister of Economy, the Chairperson of the Anti-Corruption Chamber of the Court of Cassation, and the Member of the Supreme Judicial Council were appointed to the Interagency Committee, further strengthening its multidisciplinary capacity. The Interagency Committee is authorized to coordinate NRAs and strategy development activities.

58. The Interagency Committee is supported by a working group, whose members prepare the working materials and are in charge for the implementation of its decisions. The Interagency Committee meets on average twice annually; and can meet in an extraordinary session at the request of the Chairperson or of any member on any matter or topic pertaining to AML/CFT. In parallel, the Working Group meets on a periodic basis, particularly when preparatory work is required ahead of the Interagency Committee's sessions. Such preparatory work may include conducting studies, performing in-depth analyses, or collecting relevant information to ensure informed discussion of specific issues. Minutes were provided of three Interagency Committee meetings, where issues in relation to NRA and issues of policy level were discussed.

59. When addressing issues that concern various sectors whether related to SRBs or other entities, the relevant parties were invited to participate in sessions of the Interagency Committee. For instance, in 2023, the Chamber of Advocates and the Chamber of Advocates and Expert Accountants were invited to take part in discussions regarding a study on the necessity of registering DNFBPs that currently lack supervisory authorities. In another case, in 2024, the Cadastre Committee was involved in the discussion concerning the analysis of risks associated with the real estate sector.

60. Based on the decision of the Interagency Committee, separate Working Groups are established in case thematic issues arise in the field of AML/CFT/CPF.

61. Guidance documents dealing with the investigation of ML and TF cases have been prepared by the FMC and prosecutors’ office and approved by the latter. FMC led an inter-institutional initiative to analyse the emerging and rapidly evolving risks associated with the VAs sector. This involved collaboration with the Police, the NSS, and the IC to identify VASPs mentioned in criminal reports, as well as the types of criminal activities commonly conducted through VAs. The FMC worked with the supervisory authority (FSLD) and financial institutions (banks, MVTS). Authorities reported that as a result of this strategic analysis there was an improved ML risk understanding in relation to the VAs

sector, sharing of information about domestic (detected but unregistered) and foreign VASPs, with banks and LEAs. However, the AT notes that the findings of the study of transactions involving VAs through the financial system was not disclosed to private-sector representatives and it can be used by member agencies solely for official purposes.

62. The implementation of the National AML/CFT/CPF Strategy for 2025 to 2028 and the action plan are being monitored semi-annually where the progress on implementation is discussed within the Interagency Committee.

1.6. National co-ordination and cooperation for operational purposes

63. Armenia facilitates operational cooperation and coordination through the framework of a dedicated Working Group within the Interagency Committee as explained in the previous core issue. Authorities reported that the Committee can also meet at the request of the Chairperson or of any member of the Interagency Committee on any matter or topic pertaining to AML/CTF/CPF including operational matters. Authorities reported that in parallel, the Working Group can meet on a periodic basis, where the discussions held are in relation to the Interagency Committee's sessions.

64. MOUs are in place with domestic competent authorities to ensure the timely exchange of information. Sensitive data and information are exchanged through the Financial Intelligence Data Exchange Platform which is a secured platform. FMC reported that information is routinely shared through this secured platform.

65. As a result of this cooperation several key documents were formulated that fed into operational activities. For example, a technical guidance on the investigation into TF offences was the result of an exercise initiated by the FMC together with the prosecutors' office, and the NSS. These are all commendable results, that reflect the use of cooperation and coordination to fight ML/TF at the policy making level. However, the AT does not consider that this is a mechanism that ensures proper and regular cooperation and coordination at the operational level in ML and TF cases where interagency work is facilitated.

66. Based on the on-site discussions, authorities indicated that most of the operational cooperation is on a case-by-case basis with the FMC being the key player and cooperating with different LEAs, supervisory authorities, and the tax authority, and where such cooperation is done through working groups set up under the auspices of the Interagency Committee.

67. Operational cooperation among LEAs commonly focuses on investigative assistance depending on the cases. For example, Armenia reported that in large and complex criminal cases, joint investigative groups were formed for these specific cases that involved multiple LEAs.

68. Therefore, it appears there is an element of operational cooperation where the main trigger of the initiation of cooperation is the FMC. However, there are no formal typology or intelligence-sharing mechanisms to ensure systemic operational information exchange between LEAs and intelligence bodies. The interagency framework should be further enhanced to ensure that cases are jointly initiated, merged, or developed, where all the possible sources of information are exploited and synergies created (for example, exploiting the possibility to initiate a domestic investigation from incoming MLAs). This is necessary in order to ensure the proper detection and investigation of ML and TF and to avoid duplication of efforts and missed opportunities (as also explained under IO7).

Chapter 2. International Co-operation

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

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Armenia to a large extent provides constructive Mutual Legal Assistance (MLA) and extradition, across a range of requests. There are two central authorities responsible for delivering and seeking MLA: the General Prosecutors Office (GPO) in the pre-trial stage and the Ministry of Justice (MoJ) in the trial stage. Limited statistics are available on some aspects of international cooperation (underlying criminality, response times).

b) The overall feedback received concerning MLA and extradition, in the terms of quality, effectiveness and timeliness of assistance, was positive with shortcomings noted in relation to responses times in particular cases. The time needed for executing the request may be influenced by factors such as incomplete requests, case management processes and specific requirements (i.e., translation, domestic distribution). Prioritization of requests is mostly based on the personal experience of the authorities and urgency indicated by the originator.

c) The authorities have demonstrated that they proactively seek MLA in key complex ML cases. Concerns remain whether MLA in other investigations involving ML and specific predicate offences (i.e., drug trafficking) are sent on a systematic basis, due to the tendency to focus on the domestic component of the offence. MLA is used to some extent for asset recovery, with only two confirmed cases of seizure of assets of illicit origin abroad.

d) LEAs provide and to a different extent seek other forms of international cooperation in pursuance of predicate offenses and ML using a wide range of channels. From the cases with a cross-border element presented to the AT it seems the authorities did not fully undertake a proactive approach to seeking intelligence from foreign counterparts. So far, Armenia has not been invited to nor initiated joint investigative teams concerning cross-border complex ML.

e) The FMC provides good-quality intelligence to its foreign counterparts in a timely manner. It has also suspended a transaction on request from another FIU, securing the proceeds of crime. In terms of proactively requesting information from partner FIUs, a modest number of outgoing requests was noted, raising questions whether the foreign nexus is fully considered. The FIU supported LEAs in obtaining information from foreign jurisdictions.

f) The CBA (FSLD) is active in seeking and providing informal cooperation to foreign regulatory authorities, focusing largely on fitness and propriety checks and supervision. The cooperation of non-financial supervisors is limited, primarily due to the domestic nature of the entities subject to oversight and extent of supervisory activities conducted.

Key Recommended Actions (KRA)

No KRAs

Other Recommended Actions

a) Armenian LEAs and the FIU should seek more proactively and systematically all forms of international co-operation, and send requests on asset recovery, where proceeds of crime are moved abroad.

b) The GPO and MoJ should improve the efficiency of handling incoming MLAs by enhancing and digitalizing the existing case management systems for processing and monitoring the timely execution of international cooperation requests. Written procedures should be introduced for prioritization of incoming MLA requests, in line with the main ML/TF risks faced by the jurisdiction.

c) Armenian authorities should collect more detailed statistics on formal and informal international cooperation (such as the jurisdictions involved, type of crime, average response times and the nature of information requested), which would allow to map the current state of cooperation and support its enhancement.

Overall conclusion on IO.2

Armenia generally provides good-quality and effective MLA, including extradition. Feedback on the quality and timeliness of this assistance is positive, though some delays occasionally occur due to incomplete requests, internal processing, or translation needs.

While authorities proactively seek MLA for complex money laundering (ML) cases related to corruption, they less frequently do so for other associated predicate offenses, such as drug trafficking, due to a focus on domestic aspects of the criminal activity.

LEAs and the FMC provide and to a various extent seek other forms of international cooperation in pursuance of predicate offenses and ML using a wide range of channels. The authorities did not fully undertake a proactive approach to seeking intelligence from foreign counterparts.

The CBA (FSLD) is active in seeking and providing informal cooperation to foreign regulatory authorities, focusing largely on fitness and propriety checks and supervision. The cooperation of non-financial supervisors is limited due to the domestic nature of the entities subject to supervision.

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

69. International cooperation is an important component Armenia's AML/CFT system. The jurisdiction's risk profile is shaped by a mix of domestic predicate crimes, cross-border flows, and sectoral vulnerabilities. Cross-border crimes include fraud, corruption, smuggling of narcotic drugs, psychotropic substances, their analogues, derivatives, or precursors and tax evasion. Connections with high-risk jurisdictions are relatively limited and most cross-border flows are related to normal economic activity and diaspora links. Predicate offenses with cross-border elements do not significantly increase the country's overall ML risk exposure, although the AT believes the risk impact of criminal activities

carried out by transnational organised criminal groups should be further explored by the authorities (see IO.1). Since the last MER in 2015, Armenian authorities have taken steps to improve the quality of the assistance provided to foreign counterparts and introduced a more proactive approach to seeking information abroad. Efforts have been also made to improve the collection of relevant statistics.

70. The assessment of the effectiveness of the measures in place was based on statistical data provided, interviews with the relevant authorities, discussed case studies and feedback from the global network. Relevant findings from related immediate outcomes were also taken in account to support the conclusion.

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

2.1.1. Providing evidence and locating criminals

71. Armenia has a sound legal framework for MLA, on the basis of which it provides mutual legal assistance to a variety of jurisdictions with which it has entered into multilateral (treaties) and bilateral agreements. Cooperation is most commonly provided on the basis of the European Convention on Mutual Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention), UNTOC, UNCAC, the Minsk, Chisinau and Budapest Conventions. MLA or extradition can be provided on an ad hoc basis (without a prior agreement) subject to the principle of reciprocity. The authorities have used these principles to enter into cooperation with jurisdictions such as, inter alia, Japan, Malaysia, Singapore, India and Hong Kong.

72. Armenia has established two central authorities responsible for overseeing the execution of MLA and extradition requests, in order to ensure their proper handling. The GPO is responsible for handling incoming MLARs and extradition requests in preliminary stage, whereas the MoJ has the capacity to process foreign inquiries for assistance associated with the trial stage. The GPO handling the bulk of incoming requests has 7 staff members dedicated to the task, while the MoJ has 11 people. The GPO also has within its structure the Department for Confiscation of Property of Illicit Origin, with 10 prosecutors, who are in charge for ensuring international legal cooperation on civil forfeiture matters.

73. In the period under review, the GPO received a total of 963 MLARs, of which at least a total of 355 MLARs involving TF (1 request), standalone ML, ML together with associated predicate offences and sole predicate offences. The MoJ received altogether 414 requests, but no distinction concerning specific offences was made. In the case of both the GPO and MoJ, the overall number of incoming requests has been gradually increasing between 2020-2024. The MoJ keeps aggregated statistics on incoming MLAs but no break-down by predicate offences is available.

74. The vast majority of requests originate from the Russian Federation and Türkiye. Data on incoming MLA requests provided by the GPO indicates that the main underlying offences are various types of fraud, followed by corruption and tax evasion this in line with the country ML risk profile (see IO1).

Table 2.1. Incoming MLA requests by offence (GPO)

Offence	2020	2021	2022	2023	2024	Total
ML Standalone	**5**	**7**	**8**	**4**	**4**	**28**
ML associated with[39]						

[39] It should be noted that the discrepancy in the segregated figures is due to the fact that, within a single MLAR, several criminal offences were present simultaneously — for example, fraud, money laundering, and corruption-related offence.

Fraud	**2**	**1**	**2**	**0**	**0**	**5**
Drugs Trafficking	**1**	**0**	**0**	**0**	**0**	**1**
Corruption	**0**	**0**	**3**	**5**	**1**	**9**
Tax evasion	**0**	**1**	**0**	**1**	**0**	**2**
Organised crime	**0**	**0**	**1**	**0**	**0**	**1**
Other						
TF	**0**	**0**	**0**	**1**	**0**	**1**
Terrorism	**0**	**0**	**1**	**2**	**2**	**5**
Other predicate offences						
Fraud (incl. cybercrime, forgery of documents)	**37**	**33**	**36**	**46**	**58**	**210**
Drug Trafficking	**0**	**0**	**0**	**14**	**0**	**14**
Corruption	**6**	**4**	**14**	**16**	**2**	**42**
Tax evasion	**6**	**7**	**3**	**2**	**2**	**20**
Organised crime	**0**	**0**	**2**	**6**	**2**	**10**
Cash smuggling/breach of cross-border declaration obligation	**0**	**0**	**0**	**0**	**0**	**0**
Smuggling	**0**	**0**	**2**	**1**	**2**	**5**
Arms trafficking	**0**	**0**	**0**	**2**	**0**	**2**

75. Both the GPO and MoJ confirmed, that MLARs most often involve inquiries on financial information (financial flows, account statements), the possibility to interrogate witnesses and suspects, information about the organizations, beneficial ownership information, and the identification of assets.

Table 2.2. Top MLA requesting countries

GPO		**MoJ**	
Country	**Number of incoming MLA requests**	**Country**	**Number of incoming MLA requests**
Russian Federation	671	Türkiye	225
Poland	22	Germany	83
Latvia	21	France	22
Germany	13	Greece	9
United States of America	8	Netherlands	9
France	5	Slovenia	9

76. Incoming MLAs originate to a large from extent jurisdictions possessing an Armenian diaspora, which is broadly in line with the country's risk profile. The jurisdictions in the FATF Global Network gave positive feedback on the information or answers provided by Armenia in the framework of requests with, single responses suggesting a long timeframe needed to respond to MLARs. The oldest pending MLA dates back to 2021, which is due to the fact that there are criminal proceedings in Armenia, and the provision of international cooperation may impede domestic investigation of the cases. While detailed statistics are not aggregated, the MoJ indicates the average response time to be approximately 3 to 12 months, in the case of the GPO 4 to 6 months, which can be considered appropriate.

77. The identified longer response times in specific cases may be due to a series of factors. In some

cases, additional information is also required from the requesting jurisdiction, which may take a long time to obtain. Representatives from GPO and MoJ highlighted, that they communicate the status of the inquiry to the senders and signal any need for additional information without delay.

78. In general, incoming requests are assessed for completeness, legal compliance, and relevance under the CPC and international agreements before they are sent to the responsible competent authority for execution. Both authorities have indicated different case management systems used to process and monitor the incoming requests. While both authorities have electronic case management systems in place, they would benefit from further enhancement, in the case of the MoJ, part of the efforts to monitor progress of executing requests is still done on paper. Prioritization of MLARs is not formalized in any procedure but based on the experience of the staff handling the request, which would pursue cases marked as urgent, suggesting a specific timeframe for execution or associated with cybercrime, which does not give consideration to the main ML/TF risks the jurisdiction faces or cases concerning asset recovery.

79. In the period under review there has been a steady transition from MLARs being received by the GPO using diplomatic channels to the use of email to transmit requests. This evolution was triggered by limitations introduced during the COVID 19 Pandemic and the development of lists of contact points for the purpose of cooperation under specific treaties. While the MoJ still receives a lot of inquiries via diplomatic post, urgent cases are now also transmitted via email, which has allowed to save time.

80. The execution of incoming requests on the domestic level is monitored by the central authorities. The GPO assigns a prosector responsible for handling the necessary activities. The MoJ verifies the status of the request every three months.

81. While the GPO and MoJ have indicated that each request is analysed with the view of the need of taking further action on the domestic level (outside the execution of the request), no cases have been provided to demonstrate proactively initiated investigations into persons and activities stemming from MLARs (see IO.7).

82. The AT did not identify cases of unreasonable refusals to MLA requests from other jurisdictions. The authorities engage with foreign counterparts through several platforms – both formal and informal in order to consult the process of obtaining legal assistance from Armenia. On several occasions consultation took place after receiving the requests in order to organize the execution of the proper part, prior to receiving additional documents.

83. Feedback from the global network indicated Armenia has on some occasions refused to provide mutual legal assistance to a foreign authority on grounds of the possible application of dual criminality (1 request) or the lack of a bilateral and multilateral agreement (one request). The authorities have provided explanations on the handling of these cases, which the AT finds legitimate. One jurisdiction noted that cooperation was refused on a basis that was not communicated properly. Further guidance and upfront communication with the sending authorities would allow the central authorities to mitigate such situations.

2.1.2. Extradition

84. In the period under review, Armenia has received in total 349 extradition requests, out of which around 30% were refused. Out of the 207 requests submitted to the GPO only 3 concerned ML and 2 TF. The refusals are primarily triggered by cases of dual criminality, and legislation forbidding the extradition of Armenian citizens. Other situations can concern the application of the statute of limitations and precautions as to protection of the rights of individual concerned. In case when the accused is the citizen of Armenia (who according to the law cannot be extradited), the GPO can initiate further criminal prosecution against the person on the basis of the relevant international treaties. The authorities noticed 100 such cases in the period 2020-2024. The authorities indicated that the average

time for execution of extradition requests is 11 months, which is reasonable to the AT. The need to translate the document into Armenian (which can take at least 6 months) is a factor delaying the execution. To address this, in 2025 the Ministry of Justice concluded several service contracts with translation companies to streamline the provision of translation services in the field of international legal assistance.

Table 2.3. Incoming extradition requests received and refused

Year	GPO		MoJ	
	received	Refused	received	Refused
2020	20	2	13	9
2021	22	4	9	4
2022	38	5	19	13
2023	54	5	52	20
2024	73	11	49	26
Total	**207**	**27**	**142**	**72**

Box 2.1. Swift execution of extradition request

In 2024 an extradition request for a person wanted for a "call-centre" fraud (recently widespread type of cybercrime) in especially large amount was received. The total amount of damage in the criminal proceedings was 23,793,000 euros, and 487 people were involved as victims. In just 8 months, the organization had earned (at that moment) 49,000,000 USD illegal income.

By overcoming the complex extradition process and granting the petition in 8 months, the GPO supported foreign counterparts in fight against modern cybercrime, and the accused was extradited.

2.1.3. Facilitate asset recovery

85. Armenia receives requests facilitating potential asset recovery in ML cases, which highlights the transnational element in key ML risks identified by the jurisdiction. Data available from the GPO indicates Armenia has received at least 40 requests involving identification and tracking of assets (incl. 16 ML, 13 - fraud, 4 - drug trafficking, 2 - corruption, 1 – tax evasion) 4 requests concerning freezing/seizing of assets (2 concerning ML).

86. According to the GPO and MoJ, up till now the authorities have not identified assets in Armenia belonging to the individuals in question, that could be subject to seizure or confiscation. The same is applicable to requests involving civil asset forfeiture. The AT has no evidence to challenge this conclusion, however, the difficulties noted in LEAs' capacity to perform financial analysis, and access to financial information (see IO6 and IO7) might impede the effective tracing and identification of assets located domestically.

2.2. Seeking appropriate and timely mutual legal assistance and extradition

87. Armenia seeks international mutual legal assistance in ML and predicate offences with the assistance of the same central authorities as for processing incoming requests – the GPO and MoJ. The authorities were aware of the value added of international cooperation and provided examples of cases with positive outcomes, including in complex ML cases. Nevertheless, the AT is concerned with the ability to systematically seek information abroad in ML cases of a transnational nature (e.g. drug trafficking, illegal trade of non-renewable resources, see IO1).

2.2.1. Seeking evidence and locating criminals

88. The overall number of outgoing MLA requests has steadily declined throughout the period under review. The authorities point to the earlier practices, where MLAs contained requests for information that was publicly available, as well as situations, where such information could have been obtained through informal cooperation channels. Between 2020-2024 the GPO has sent out a total of 2235 MLARs and the MoJ a further 220 MLARs. These include (as available GPO statistics indicate) requests concerning standalone ML and ML associated with predicate offences, predominantly corruption and tax evasion. The AT notes the important proportion of ML related requests in the total number of MLAs as well as the fact that the potential predicates reflect to a large extent the country risk. The AT considers the outgoing requests generally aligned with the main ML/TF risk environment in the jurisdiction while acknowledging that efforts in international cooperation concerning ML linked with drug trafficking and organised crime, cannot be considered fully consistent with Armenia's external threat (see IO1, 7 and 8).

Table 2.4. Outgoing ML related MLAs sent by the GPO

Offence	2020	2021	2022	2023	2024	Total
ML Standalone	2	12	9	4	24	51
ML associated with[40]	49	25	11	9	15	109
Fraud	1	2	0	1	1	5
Drug Trafficking	0	0	0	0	0	0
Corruption	31	22	3	5	4	65
Tax evasion	22	10	7	4	3	46
Other	8	9	1	1	7	26
TF	0	0	0	0	0	0
Terrorism	0	0	0	0	0	0

89. As reflected in Table 2.4, the number of outgoing MLARs relating to ML associated with a predicate offence has strong fluctuations over the reporting period, an increase in requests on standalone ML has been noticed, and no TF requests have been sent. However, there are concerns regarding the accuracy of this data, as it does not align with the number of ML investigations and prosecutions, both for standalone cases and those associated with the high-risk predicate crimes, which is significantly lower in some cases (see IO7). For example, the total number of standalone ML investigations over the reporting period is 16 (compared to 51 outgoing requests indicated in Table 2.4), with the first one initiated only in 2022; there were only 13 ML investigations associated with tax evasion (compared to 46 requests indicated in Table 2.4), with only 2 investigations in 2020.

90. The main criminal offences associated with MLARs (general) are fraud, smuggling of narcotic drugs and psychotropic substances, computer-based illegal taking and forgery of documents, which is largely in line with the country risk profile. The number of requests associated with the smuggling of narcotic drugs has diminished over the years to a handful of requests. The authorities indicate that this is caused by the fact, that the vast majority of these requests were sent to jurisdictions, where their purchase is legal, which resulted in no valuable information obtained.

91. The most common types of assistance sought under the MLA procedures are the collection and sharing of evidence (mostly bank records and financial documents), corporate and shareholder information, witness statements or testimonies and certified copies of official documents. The majority of MoJ requests are sent to France, whereas GPO processed MLARs are sent to the Russian Federation,

[40] It should be noted that the discrepancy in the segregated figures is due to the fact that, within a single MLAR, several criminal offences were present simultaneously — for example, fraud, money laundering, and corruption-related offence.

USA, France, Georgia and Germany. No joint investigation teams (JITs) were assigned to ML matters.

92. The same dedicated teams in the MoJ and GPO ensure that all outgoing international cooperation requests are prepared in accordance with relevant legal frameworks, treaties, guidelines, and include clear, complete, and accurate information. The main initiators of outgoing requests are the investigative authorities – the ACC and IC. The investigator handling the case is the person who creates the draft MLAR. The GPO make sure that the requests contain necessary details such as legal qualifications, facts of the case, and supporting documents. As a good practice, formal requests are preceded by informal requests on the FIU or LEA level. Verification is made whether the contents of the request reflect the relevant multilateral and bilateral treaties Armenia is party to. Requests are being translated into the required language of the requested country. Close coordination with investigative bodies ensures factual accuracy and consistency. When needed, inter agency follow-up communication is maintained to provide clarifications and support execution. In complex and urgent cases – sending the request via Eurojust.

93. Members of the FATF Global network have highlighted the overall good quality of requests from Armenian authorities, with some room for improvement concerning their quality signalled by individual jurisdictions. Both the GPO and the MoJ have identified a gradual increase in the quality of outgoing mutual legal assistance requests, signalled by lower numbers of received follow ups from recipients. This is supported by available statistical data, which shows a gradual decrease of the number of requests subject to returns and refusals.

94. While no track is being kept of the average time to execute outgoing requests, the GPO and MoJ recall jurisdictions which are uncooperative or take a long time to respond. In such cases a reminder is sent, and the authorities try to contact their counterparts. In cases where there are no agreements (bilateral and multilateral) in place, the authorities try to establish formal ties.

2.2.2. Extradition

95. Armenia effectively seeks assistance to extradite criminals in ML and associated predicate offences. In the period under review Armenia reported 110 extradition requests, 7 of which concerned ML. Around 50% of the requests were granted while 30% refused or returned (remaining cases are still underway). In extradition matters, the authorities commonly seek assistance for the following: the location, arrest, and surrender of fugitives wanted for prosecution or execution of sentence. Extradition-related feedback is commonly provided, especially in cases where requests are delayed or refused. Partner countries typically clarify the grounds for refusal (e.g., dual criminality, procedural deficiencies, or human rights concerns).

2.2.3. Seeking to facilitate asset recovery

96. According to the information provided by the GPO, the majority of asset recovery related requests sent by Armenia concerned ML cases with a total of 6 such requests issued for freezing/seizing of funds in criminal proceedings. A further 5 asset recovery MLARs concerned criminal proceedings concerning corruption and one involved fraud, which can be considered mostly in line with the country risk, given the modus operandi associated with the main ML risks in Armenia. At the same time, the AT is not convinced asset recovery is proactively pursued as a policy objective in all ML and proceeds generating cases with a cross-border nexus (see IO.8).

97. As in the case of incoming requests, MoJ does not gather detailed statistics in order to distinguish MLARs associated with asset recovery.

98. The authorities have demonstrated the ability to request assistance from foreign counterparts for freezing/seizing proceeds of crime in key ML cases. While none of the MLARs sent out have been finalized, there are indications that the authorities will be able to repatriate some of the illicit assets transferred abroad.

99. None of the requests concerning civil asset forfeiture ended with a positive response.

Box 2.2. Seizure of assets abroad

Person X, being the director of Company A and B, intentionally failed to pay particularly large amounts of taxes by entering obviously false data in the calculations submitted to the tax authority as a result of the entrepreneurial activities carried out by the aforementioned companies during 2004-2014. In addition, he organized the process of not paying taxes in particularly large amounts by entering obviously false data in the calculations submitted to the tax authority in 2006 as a result of the entrepreneurial activity carried out by the company C, which he actually owned since 2002, as a result of which he assisted officials in receiving bribes in particularly large amounts in order to carry out actions in favour of Person Y, assisted a high-ranking official in legalizing the money obtained through criminal means, and also committed money laundering in particularly large amounts within the group with prior consent.

Based on the requests for legal assistance, the Slovak Republic seized funds of 380.000 € in 2022. Additionally, in 2023 Slovak Republic based upon Armenian request executed seizures of a car, real estate, parking lots and funds of 23.674 €.

Box 2.3. Seizure of real estate abroad

The case highlights how high-level corruption and abuse of official positions were facilitated through intricate schemes involving concealment, fictitious transactions, and the use of companies to launder the proceeds of crime.

This case concerns large-scale embezzlement, bribery, tax evasion, and money laundering involving a former high-ranking Armenian official and his close relatives. The criminal investigation was initiated based on information obtained during the course of a separate criminal proceeding and formalized through an investigator's report. Throughout the investigation, extensive inquiries, interrogations, and analysis of financial data (including information protected by banking secrecy laws) revealed that the PEP and his relatives exercised de facto control over a network of companies in Armenia and foreign jurisdictions, while concealing their ownership through relatives and affiliated individuals.

International cooperation played a crucial role in advancing the investigation. Numerous mutual legal assistance requests were sent to the United States, France, Austria, Germany, Cyprus, and other countries. In particular, collaboration with U.S. and Austrian authorities facilitated the retrieval of key financial documents. As a result, a mansion belonging to the PEP's family, located in the United States and valued at approximately USD 36 million, was seized, sold at the highest market price, through a U.S.-initiated investigation and civil forfeiture action pursued before U.S. courts.

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

100. Informal cooperation is regulated by international treaties, multilateral or bilateral agreements, MoUs. or conducted ad hoc. Direct and informal international cooperation is a usual practice before engaging in mutual legal assistance. Feedback received from the FATF Global Network on the provision of other forms of international cooperation was generally positive.

2.3.1. FIU

Incoming

101. International cooperation requests in the FMC are handled by the Analysis Unit responsible also for conducting operational analysis and responses to domestic requests. The Unit has a total of 12 employees. The FMC uses two secure information channels – the ESW for cooperation within the

Egmont Group and the CIS FIU network for cooperation between FIUs of the Commonwealth of independent states (CIS). The FIU has signed a total of 34 MoUs with foreign counterparts.

102. The international co-operation provided by the FMC is timely and effective. This conclusion is based on the analysis of both the information requests; the spontaneous disseminations and the feedback received from the Global Community.

103. During the period under review the FMC received a total of 205 requests from foreign FIUs. The highest number of requests came from the Russian Federation, Latvia, Cyprus, Kazakhstan, Moldova, and Ukraine. These requests mainly related to the involvement of Armenian residents in various criminal schemes in the respective countries, including ML, tax abuse, drug trafficking, and fraud, as well as requests regarding different ML/TF or other higher risk criteria sent to all FIUs in the Egmont Group/CIS. The average response time was in general below 30 days. In urgent cases responses were provided within 5 days. The FIU has used the suspension mechanism on the request of a foreign FIU on at least one occasion. The sending FIUs usually request information on bank accounts and other assets held by the subjects of analysis, on the transactions through the bank account, STRs, ML investigations and/ or criminal records, data on movable/immovable property, etc. The quality of responses was considered good. General prioritisation mechanisms for operational analysis are used for cases opened on the basis of international requests. No refusals were noted.

Table 2.5. Incoming requests to FIU

Incoming requests to FIU	2020	2021	2022	2023	2024
- ML	7	17	6	15	7
- TF	0	3	1	1	0
- Predicate offence					
Tax evasion	4	11	8	10	2
Fraud	5	7	5	4	9
Corruption	1	6	2	2	2
drug trafficking	3	4	2	4	0
ML/TF and other higher risk criteria	4	6	5	12	11
Other	2	8	4	4	1
Total	**26**	**62**	**33**	**52**	**32**

104. During the reporting period, the FMC also received 95 spontaneous disseminations from foreign FIUs. These disseminations generally fell into three main categories: notifications sent to a large group of FIUs simultaneously, without specific country context, follow-up notifications, where the FMC had previously submitted a request to a foreign FIU and notifications that contain negative information from media sources about Armenian residents, citizens, or individuals of Armenian ethnicity.

105. Particular requests and spontaneous disclosures have triggered FIU analysis, which further led to a total of 15 disseminations concerning potential ML/TF to domestic LEAs (see IO.6).

Outgoing

106. Outgoing requests are triggered in the course of operational analysis when there is a need to substantiate the reliability of a particular hypotheses put forward as a result of a summary of the preliminary information in the case. To send a request to a foreign FIU, the analyst responsible for the case must first enter a draft letter into the CMS and submit it to the Head of the Analysis Division of the FMC for consent. If needed, the Head of the Analysis Division of the FMC will coordinate with the Head of the International Relations Division of the FMC before forwarding the draft to the Head of the FMC for final approval. Once approved, the Head of the FMC instructs the Head of the International Relations Division of the FMC to send the request.

107. The number of outgoing requests (88 requests in 70 cases between 2020-2024), while broadly in line with the jurisdiction's risk profile, is relatively low. The impact of the low number of outgoing requests is even more evident when considering that 38 were triggered by LEAs. This can signal a potential reluctance to pursue the foreign element of the ML offence, where a notification to an intelligence body is already substantiated based on other information obtained domestically.

108. Given the number of STRs[41] involved transactions with a broadly defined "foreign nexus" where both residents and non-residents of Armenia were involved, a more proactive stance should be taken in seeking international co-operation.

109. The FIU has drafted guidelines for using FIU intelligence in drafting MLA requests. As a result, operational information received from foreign FIUs was incorporated into some MLAs.

Table 2.6. Outgoing requests and disclosures to foreign FIUs

	2020	2021	2022	2023	2024
Requests to foreign FIUs	43	5	25	4	11
Disclosures to foreign FIUs	5	3	0	3	2

Box 2.4. International cooperation on cross-border ML scheme involving PEPs

In a criminal proceeding investigated by the ACC, the PEP and his wife were involved as defendants under a ML case for legalizing approximately 2 million EUR obtained through criminal means.

In 2020, the FMC received a request from the ACC concerning the PEP and affiliated subjects. According to information provided by the ACC, the former PEP, through affiliated natural and/or legal persons, conducted financial transactions potentially involving illicitly obtained assets, including the purchase of real estate abroad. The ACC requested financial transaction data for approximately 20 natural and/or legal persons.

Based on the ACC request, the FMC conducted a comprehensive analysis of the PEP and affiliated subjects and presented a summary of the findings. Among the key elements revealed in this complex investigation were cross-border transactions with Greece. Consequently, the FMC made requests to the FIU of Greece. The combined analysis established the following regarding the PEP's spouse:

- Approximately EUR 400,000 was deposited in her Armenian bank account and subsequently transferred to her Greek bank account;
- The total turnover of the Greek bank account over a two-year period amounted to EUR 423,000, which were then transferred to two other bank accounts in Greece in order to purchase real estates;
- She imported approximately EUR 250,000 in cash from abroad;
- She purchased and/or held a total of five real estate properties in Greece.

Detailed information on the identified assets (e.g., property addresses, purchase dates, related bank transactions, etc.) was transmitted to the ACC to support, among other actions, the submission of a mutual legal assistance request.

The information was utilized to prepare a mutual legal assistance request sent to the competent authorities of the Republic of Greece.

The case is currently subject to two parallel judicial proceedings: one criminal and one non-conviction-based forfeiture procedure. A decision to freeze real estate and personal accounts in Greece has been sent to Greece.

[41] 367 STRs in the period between 2021-2023 in accordance with the ML/TF NRA. These STRs represented about 59% of the total funds involved in all STRs in that period. In the case of STRs that triggered a dissemination to LEAs, 20% included a foreign nexus (for more details see IO.1).

110. FIU requests were in general considered good quality. In the rare cases where additional information was requested regarding the request sent by the FMC, further assistance was swiftly provided (in one case - also via remote meeting organised) and the responses were obtained.

2.3.2. Law enforcement agencies

111. In the period under review, LEAs engaged in international cooperation to combat ML/TF crime in key cases. The limited availability of statistics on informal requests for some LEAs (NSS, MIA) makes it challenging to fully ascertain the level, to which assistance is regularly sought and provided, and meetings with the authorities onsite indicated, that international cooperation on ML, including asset recovery is not approached in a systemic manner. The authorities demonstrated the proactive approach on specific cases

112. LEAs, use a wide range of channels for cooperation, including INTERPOL, CARIN, UNODC GlobE Network, and OECD Law Enforcement Network for Eastern Europe and Central Asia, networks based on multilateral treaties and direct communication with foreign counterparts. The authorities have signed a series of MoUs with foreign authorities (inter alia US agencies, the European Union Drugs Agency and Europol), to facilitate cooperation and training.

113. Incoming requests mainly require basic information on bank accounts of individuals, legal entities and organizations, as well as information on beneficiaries, information on the availability of immovable and movable property. LEAs advise the use of formal channels (MLA) in order to be acquire information subject to banking confidentiality, due to the necessary judicial authorization.

114. Incoming requests received through Interpol channels are mostly addressed within a 30-day period. If the requests contain unclear or incomplete information (e.g., incorrect name of a person, legal inaccuracies), the relevant LEA seeks clarification through official or unofficial channels before acting. None of the requests received by LEAs through informal channels led to the triggering of a ML investigation (see IO.7).

115. Outgoing inquiries mainly request information on the availability of bank accounts, immovable and movable property of natural persons. In the case of investigative authorities (IC, ACC) long response times of foreign counterparts and silent refusals remain a challenge, which however does not remain on Armenia's side. In such cases LEA representatives tend to engage in informal contacts and set up meetings to put emphasis on the execution of their requests.

116. Given the absence of detailed statistics for LEAs and deficiencies identified under IO.7 and IO.8, the AT cannot conclude that the informal co-operation carried out by the Armenian LEAs and is fully effective.

Authority responsible for asset recovery

117. While there is no authority acting as dedicated asset recovery office in Armenia, the GPO has a special Department for the Confiscation of Property of Illicit Origin with 10 prosecutors, which is responsible inter alia for ensuring international legal cooperation on civil forfeiture matters. Apart from MLAs, the Department also uses informal cooperation through the CARIN network. The Department received 19 requests and sent 46 such requests during 2020-2024, which appears to be commensurate with the MLA requests. However, no assets were traced or identified in Armenia or abroad.

2.3.3. Supervisors of FIs, VASPs and DNFBPs

118. The CBA (FSLD) as the financial supervisor provides and requests assistance from its foreign counterparts. During the period from 2020 to 2024, the assistance requested primarily pertained to information relevant to conducting fit and proper assessments for supervisory purposes (27 cases), as well as to basic and beneficial ownership information (15 instances). In some requests, (4) account-

related information was also included. Most requests are made through the IOSCO channel. The CBA has implemented a case management system, which is employed to monitor and track request handling. The average timeframe for response was 1 month. No refusals were noted. Where appropriate, the CBA engages in pre-response consultations or follow-up dialogue with the requesting authority to clarify any ambiguities in the request or to confirm the specific information needed. CBA has established formal relationships with the supervisory authorities of 17 jurisdictions through signed MoUs. The lack of a bilateral agreement does not exclude cooperation with foreign counterparts. A questionnaire was distributed to receive feedback from recipients of data from the CBA.

119. In the context of outgoing requests, the CBA mainly requests information necessary for fit and proper assessments in the context of supervision (14 instances), along with basic and beneficial ownership data concerning legal persons and legal arrangements (7 cases).

120. The SRC in its capacity as the supervisory authority responsible for monitoring gambling activities, casinos, and lotteries has in one case requested information regarding the volume of financial transactions, the methods of transfer—whether cash or cashless—and the documentation of services provided between a company registered and operating in Armenia and companies supplying it with gaming services in order to verify whether those companies are duly registered and to determine the volume and nature of the transactions conducted by the Armenian company.

121. In the case of the MoF (responsible for performing screening of qualified holders, BOs and managers, at the market entry stage of casinos and online gambling operators), due to the lack of necessity, no inquiries were made to foreign authorities.

122. Due to the FMC taking up its supervisory role of certain DNFBP sectors in 2023 and the fact that the sectors under FMC's supervision did not have identified international exposure, the authority has not had any experience in conducting international cooperation so far.

2.3.4. Customs and tax authorities

123. The SRC provides regular assistance and information to foreign competent authorities upon request. In the field of tax matters this includes inter alia: (i) tax information on individuals and legal entities, including income declarations, tax filings, and audit results; (ii) basic and beneficial ownership information of legal persons and arrangements, in coordination with the State Registry and other competent authorities; (iii) account information and financial data (when available through domestic procedures) (iv) information on real estate and vehicles through interagency cooperation with cadastre and transport authorities; and (v) any other relevant documentation required for assessing tax liabilities or investigating tax evasion, within the limits of domestic law and applicable international agreements. In the area of customs cooperation, assistance is provided on reported or planned activities which constitute or may constitute an operation in breach of customs legislation. This includes, among others, information whether goods exported from the territory of the applicant have been duly imported into the territory of Armenia. Requested information frequently refers on individuals or legal persons activities, to exclude their involvedness in activities that violate customs legislation. The SRC has a formalized prioritization mechanism to handle the incoming requests.

124. In the period under review, the SRCs has received a total of 445 requests and sent out 501 requests (concerning both tax and customs violations). Requests on tax matters, on average can take around 180 days, in line with the OECD standard. The number of incoming requests concerning potential ML remains unknown, whereas 5 outgoing requests could be attributed to money laundering, which would be fairly low given the risk of ML stemming from tax evasion in Armenia. Discussions held with the representatives of the Customs branch of the SRC indicated, that they do not in all cases proactively cooperate with their counterparts in cases of identified smuggling of cash or trafficking of drugs coming into Armenia, leaving such actions to other authorities.

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

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

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The CBA has controls in place to prevent criminals and their associates from entering the regulated market and applies a unified approach across all financial institutions (FIs). It is empowered to reject or revoke licenses and has exercised these powers when adverse information was identified or brought to its attention. Recent rules require the annual re-evaluation of shareholders, BOs and managers of FIs. Reporting entities are also required to keep this information up to date and inform the CBA of any changes. The scope of monitoring, including the frequency of criminality checks, is to be defined by each FI through internal regulations.

b) VASPs and non-public investment funds and their managers remained outside the CBA's licensing and supervisory regime throughout most of the assessment period. This gap was addressed through the adoption of a new regulatory framework in 2025 (before the onsite).

c) The CBA demonstrates a comprehensive understanding of ML/TF risks across the financial sector. At institutional level, risks for core FIs are assessed through a structured model combining systemic and institutional elements, supported by extensive data collection. For smaller FIs, such as currency-exchange offices, risk is assessed through supervisory judgement. At group level, risk assessment is performed mostly from a prudential point of view.

d) AML/CFT supervision by the CBA is guided by dedicated procedures and methodologies for banks and non-bank FIs, introduced gradually from 2020 and continuously improved since. These frameworks prescribe permanent (annually or quarterly) off-site risk analysis and compliance scrutiny for all material sectors. More in depth cyclical on-site inspections were recently introduced, with frequency based on ML/TF risk of each entity. For much of the assessment period, inspections were triggered by specific events or intelligence or took the form of sectoral thematic reviews.

e) Most banks demonstrate a comparatively good understanding of risks and are able, to a large extent, to articulate those most relevant to their operations. Other FIs tend to refer to broader national threats, with a limited understanding of how these risks might materialise in their business context. Across the sector, the distinction between ML and TF risks remains weak. Most entities assess the overall TF threat as low, consistent with the NRA, with comparatively limited attention given to TF-specific risk factors and scenarios.

f) All FIs demonstrate awareness of their AML/CFT obligations and have internal controls in place. More material FIs generally rely on third-party technical solutions, particularly for remote onboarding and ongoing customer screening and monitoring. Smaller FIs tend to leverage banks' customer due diligence measures, often treating the existence of bank accounts as mitigating measure. STR reporting levels remain relatively modest across the sector, with FIs generally applying a high threshold for identifying and reporting suspicious activity.

g) The CBA actively engages in supervisory outreach and follow-up actions, providing structured feedback and guidance to FIs. Material FIs receive institution specific feedback through annual "Dear CEO" letters. The FMC has also been actively involved in providing guidance and assignments to the financial sector, tailored to specific issues such as transaction types and CDD. The CBA has demonstrated an improved ability to impose proportionate sanctions, including fines, license revocations, and the removal of managers, notably since introducing new full scope on-site inspections based on ML/TF risks, which have led to improvements in compliance, particularly within the banking sector.

Key Recommended Actions (KRA)

a) The CBA should complete the first full cycle of risk-based on-site inspections, covering the entire population of each FI type within the prescribed timeframes and make stronger use of the extensive data it collects to guide targeted, risk-driven inspections.

Other Recommended Actions

a) The CBA should introduce clear requirements for FIs to conduct periodic re-assessments of the fitness and propriety of their key function holders, including criminal record checks, with defined minimum frequency to supplement CBA's own annual screening and address gaps in coverage, particularly for non-resident managers and board members.

b) The CBA, together with the FMC, should continue outreach activities, especially for smaller FIs to strengthen their understanding of AML/CFT obligations, with particular emphasis on STR reporting requirements. In addition, further sector-wide outreach is needed to improve the understanding and identification of PEP associates and related reporting obligations across all FIs.

c) The CBA should continue to apply its enforcement measures when deficiencies are discovered. Furthermore, the CBA should ensure that sanctioning decisions are made public with sufficient detail, including relevant findings, in order to maximise their deterrent effect and promote sectoral awareness of compliance expectations.

d) The CBA should further strengthen supervisory follow-up mechanisms, including through systematic tracking of remedial actions and repeat findings, in order to better assess whether supervisory interventions result in sustained improvements in compliance.

Overall conclusion on IO.3

Armenia has taken important steps to strengthen AML/CFT supervision and implement a risk-based approach, including the introduction of cyclical onsite inspections during the latter part of the assessment period. The CBA has developed structured methodologies for sectoral and institutional risk assessment, introduced annual supervisory questionnaires combined with systematic offsite inspections, and enhanced coordination with the FMC.

Fit and proper checks are comprehensively applied at market entry stage, demonstrating that criminals and their associates are prevented from penetrating the financial system. VASPs and non-public investment fund managers have only recently been included in the regulatory area of the CBA, including for licensing purposes.

The number of onsite inspections has increased in the recent period and is risk driven. However, the practical effectiveness of the newly cyclical onsite inspection framework could not yet be fully demonstrated, as most inspections during the assessment period were based on trigger events and supervisory judgement rather than systematic risk cycles.

The banking sector, which dominates the financial system, received the highest supervisory attention and shows notable improvement in compliance, driven by consistent off-site engagement, targeted inspections, and feedback mechanisms. The quality of enterprise-wide risk assessments, internal controls, and STR reporting in banks has improved, supported by sector-wide measures to professionalise AML/CFT functions. By contrast, smaller and less material FIs display a more limited understanding of risks and their AML/CFT obligations.

The CBA's supervisory actions, through off-site reviews, feedback letters, and the application of proportionate sanctions, have had a positive and measurable impact on the compliance behaviour of financial institutions, particularly banks. The introduction of published sanctions in 2024 has enhanced their deterrent effect, although the impact remains limited as publications lack sufficient detail on the nature of the breaches.

Armenia is rated as having a moderate level of effectiveness for IO.3.

125. Armenia's financial system is largely bank centered, with 17[42] universal banks, with a large proportion of local capital. Given the sector's materiality and systemic importance, the analysis under IO.3 places greater emphasis on the banking sector. Other financial institutions (credit organization, payment and e-money providers, and investment firms) are significantly less material and therefore received proportionate attention of the AT (see further Materiality of FIs, VASPs and DNFBPs).

126. Until early 2025, non-public investment funds and their managers operated outside the CBA's supervisory and licensing regime and were only required to register fund's rules, without any authorisation or fit-and-proper requirements. The introduction of a licensing framework[43] in August 2025 represents a major improvement, but its effectiveness could not yet be assessed given its recent implementation.

127. Armenia currently has no life insurance sector. At the time of the onsite visit no virtual-asset service providers (VASPs) had yet been licensed, as the recent regulatory regime was still being implemented. These sectors were therefore considered non-material and were not subject to detailed analysis for the purpose of this assessment.

128. The technological solutions- such as remote onboarding, digital identification, and automated monitoring- are now used extensively across the financial industry. These developments were examined by the AT, particularly in relation to banks, MVTS providers, and investment firms, due to their potential ML/TF implications.

129. Since the last evaluation, Armenia has undertaken substantial reforms by introducing a risk-based supervisory framework and improving the effectiveness of licensing and sanctioning mechanisms. The CBA has modernised its supervisory architecture, consolidating prudential and AML/CFT supervision

[42] The total number dropped from 18 after a merger was finalized in 2025.

[43] Investment Funds Law, Art. 8(1) – 8(4).

under a single structure with a dedicated AML/CFT risk unit. A risk-based supervisory methodology adopted in 2020 initially for banks, and later expanded to other material NBFI, underwent extensive improvements between 2023 and 2025, including the recent introduction of cyclical on-site inspections. The CBA also enhanced licensing procedures, introduced integrity and beneficial-ownership checks, and extended these controls to newly regulated sectors such as VASPs, whose licensing regime has not yet been implemented at the time of the onsite.

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

3.1.1. Market entry controls

130. The CBA, as licensing authority for all FIs, has controls in place to prevent criminals and their associates from entering the regulated market, with some entities such as non-public investment funds, their managers and VASPs only recently brought withing the licensing framework. Within the Financial Supervision and Licensing Department (FSLD), two specialized units comprising a total of 13 staff members (out of 96 staff members at the CBA in 2024.) are responsible for reviewing licensing applications and assessing the fitness and propriety of shareholders, beneficial owners and senior managers, including key function holders. Resources remained stable throughout the assessment period and are considered adequate by the AT in relation to the size of the financial sector. An increase of about 50% is projected by end of 2027, reflecting expanded supervisory responsibilities, including the recently approved licensing and supervision of VASPs.

131. While sectoral laws set out distinct licensing provisions, the CBA ensures consistency in practice through a formalized internal process set out in the Licensing Manual, which is applied uniformly across all FIs. The same fit and proper checks apply when approving changes of ownership, qualifying holding or management position. Each application involves verification of the criminal background of qualifying shareholders (10% or more direct or indirect interest), BOs and all managerial positions (see also R.26). The AT was also presented with a case involving scrutiny of an application for the acquisition of a stake of less than 10%. Although dating back to 2020, it illustrates the CBA's proactive approach.

132. For residents, CBA obtains criminal records directly from the MoI, while non-residents must provide official criminal records issued by the competent foreign authority and dully apostilled. An all-crimes approach applies in the licensing process, including non-financial offences, which are assessed on a case-by-case basis where they may provide grounds for rejecting the application. In addition to criminal convictions (in particular those that have not been expunged or cancelled), intelligence information regarding potential involvement in criminal activity is also taken into account.

133. The CBA reviews ownership and control structures as part of the licensing process. In practice, most applicants have simple and transparent ownership chains with the most complex case presented to the AT involving a general insurance company[44] with four layers between the shareholder and the ultimate beneficial owner.

134. As part of integrity assessment of applicants, the CBA complements criminal background checks with open source and database analysis to identify potential associates or links to criminal activity. As most applicants are Armenian residents, a broad range of domestic databases is used, including those of Police of the MIA (for criminal records), Credit Registry, Citizen Identification System, Judicial Information System and the registry of companies, which allows, to some extent, the identification of potential links between applicants and criminals. For non-residents, Interpol inquiries

[44] Although the example refers to a FI that does not fall under the FATF definition, the AT took it into consideration as benchmark for the analysis.

are conducted, and applicants must provide a certificate issued by the competent authority in their country of residence.

Box 3.1. Case Study – Fit and proper (criminal association identification)

In 2020, the CBA received an application for the licensing of an MVTS with a single shareholder. During the verification process, it was identified that the applicant was involved in several other companies and had business associations with multiple individuals. One of these individuals was registered at the same residential address as a person known for a criminal background.

This information was obtained through cross-checks of the judicial information system (criminal records) and the electoral system (residential address).

On the basis of these findings, the CBA concluded that the applicant could not be granted a licence due to the unacceptable risk of association with a criminal.

Source: CBA

135. The CBA also maintains close cooperation with FMC. Before granting a license, and at least annually thereafter, the CBA submits a list of individuals recorded in its licensing database to the FMC for screening against its databases, which include information from prosecutorial and pre-trial investigations This mechanism supports the identification of potential criminal associations. For non-resident applicants, commercial intelligence databases and other private sources are used to identify adverse information or criminal associations. Additional relevant checks include source of wealth and funds used for capitalisation, supported by audited financial statements, bank references or equivalent documentation, as well as the evaluation of applicant's business model and internal risk control framework.

136. On-going monitoring of the fitness and propriety of ownership and management is conducted through a multi layered approach and constitutes the main post licensing control, as licenses are granted on an open-end basis[45] (there is no system for periodic license renewal). First, any changes to BOs, shareholders, or managers require prior CBA approval, and FIs must provide annual updates on their BOs. Second, a recent amendment of the Licensing Manual provides for annual re-evaluation by the CBA of shareholders, BOs and managers. In practice, a key tool used by the CBA is the annual screening of all key individuals against different databases, including the FMC's databases, police information, other LEAs and commercial databases.

137. Third, FIs are also required to periodically verify compliance of their managers with fit and proper requirements. The depth and frequency of such analysis is not prescribed in CBA Regulations, and each FI must define these aspects in its internal acts. This is an important tool of ongoing monitoring, as about seven percent of all managers and board members of FIs in Armenia are non-residents, therefore, any criminal issues would likely not be captured by national Armenian databases used by the CBA or commercial databases. Although there is no direct requirement for FIs to include criminal record checks in this periodical monitoring, absence of convictions is one of the key components of the fit and proper test and is expected to be performed. Extracts from internal rules of banks presented to the AT show that, in practice, criminal records of key executive officials are periodically checked.

138. For BOs, FIs are required to conduct annual due diligence to identify the ultimate controller and to report any changes to the CBA, which then reviews this information and performs compliance analysis.

[45] Only in case of banks, managers are subject to re-interview every five years (see c.26.1).

139. Lastly, the CBA relies on external information and triggers, including those identified during supervisory activities.

140. The AT was presented with a case in which the CBA identified an individual who attempted to conceal a significant controlling interest in an investment company by acquiring only 9.8% of shareholding while having a secret arrangement with the manager. This case was identified during the submission of a capital increase request, following which an on-site inspection was conducted that confirmed the suspicions. The individual was subsequently required to divest the holding.

141. Criminality issues are detected and addressed, but in practice findings predominantly concern smaller or less material institutions. During the assessment period, there were three cases identified of non-compliance due to criminal nature of managers or significant participants, which were subsequently removed from office.

3.1.2. Detecting and addressing breaches

142. Statistics and case studies presented to the AT confirm that CBA's powers to reject or revoke licenses are applied in practice when adverse information is identified or brought to its attention. Between 2020 and 2024, the CBA processed a total of 174 license applications across different sectors, with rejections occurring where fit-and proper issues were identified (see Table 3.1 and 3.2). This demonstrates that market-entry controls are operational and not applied in purely formal manner.

Table 3.1. Licensing applications for FIs (2020-2024)

Entity	New licence for FI				Approval of significant shareholders and BOs			
Entity	Received	Withdrawn	Approved	Rejected	Received	Withdrawn	Approved	Rejected
Banks	1	0	1	0	36	1	35	0
MVTS	7	0	5	2	41	0	35	6
Investment companies	14	1	12	1	51	6	41	4
Credit organizations	7	0	7	0	56	4	52	0
Fund managers	65	7	58	0	12	6	6	0
Foreign exchange	75	1	71	3	205	4	195	6
Pawnshops	5	0	5	0	28	0	28	0

Table 3.2. Licensing applications of managerial positions (2020-2024)

Entity	Received	Withdrawn	Approved	Rejected
Banks	348	17	331	0
MVTS	56	6	46	4
Investment companies	125	10	112	3
Credit organizations	273	8	264	1
Fund managers	37	8	29	0
Foreign exchange	85	1	81	3
Pawnshops	23	0	23	0

143. Detection of unlicensed activity falls under the responsibility of the CBA's Business Conduct Division, which operates in accordance with an internal manual and uses automated monitoring system to scan public sources and selected online platforms. This includes the use of web crawlers, social media scanning and targeted webpage monitoring. During the assessment period, 146 cases of potential unlicensed activity were detected and referred to LEAs. The FMC also contributes to these efforts by identifying potential unlicensed activity and transmitting relevant information directly to LEAs.

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

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

144. Since 2020, the CBA has progressively strengthened its understanding of ML/TF risks across the financial sector, through the development of a risk-assessment model that now serves as the central tool for identifying both systemic and institutional ML/TF risks. The model combines inherent-risk and internal controls assessment based on data collected remotely through annual[46] risk evaluation questionnaires submitted by FIs. These questionnaires are embedded with data validation and automated ratio computation formulas and macros, which contribute to consistency and comparability of assessments across similar entities, and reduce human error.

145. Supplementary data on cash transactions and STRs is obtained from the FMC. The approach is formalised through two dedicated methodologies, one for banks and one for investment companies, MVTS providers and credit organizations. The Central Depository is also risk assessed annually. Other FIs, such as currency-exchange offices and investment funds and their managers, were assessed through supervisory judgement[47],reflecting their lower materiality and limited systemic relevance. This differentiated approach is broadly commensurate with the risk profile and size of the respective sectors.

146. Institutional inherent risk assessment relies on specific quantitative criteria, including data on active[48] customers (the most complex set of data required), cross-border transfers, geographic exposure, delivery channels (face-to-face or non-face-to-face) and products/services offered. For each criterion, the CBA calculates ratios reflecting *systemic* risks (weighted by the FI's market share) and, since 2023, also *individual* risk (specific to the institution). The combined results, which include at present 32 different risk ratios, determine the final inherent risk score for each FI.

147. For banks and other NBFIs, the datasets used are largely comparable, with adjustments for sector-specific activities. Institutions are required to submit granular information on their customer base and transactional profile, including the number of PEPs (foreign and domestic), high-net-worth individuals, legal entities with complex ownership structures, and customers from higher risk categories such as NGOs, casinos and gambling operators, or currency-exchange offices. The CBA defines complexity and risk categories centrally to ensure consistent reporting standard across all FIs.

148. The model incorporates selected NRA findings, for example by capturing the number of individual PEP customers, reflecting corruption as a key ML threat in the jurisdiction.

149. The inherent risk model applies a largely uniform ordinal scoring scale (1-3) for each criteria category, with only cash transactions benefiting from an expanded scale (1-4). The authorities advised that the division of categories to which those weights apply (for each ratio) is based on observations and risk analysis and can therefore be adjusted to capture shifts in the risk environment when needed.

150. The final design for calculating the overall final ML/TF score, on which on-site inspection frequency is based, incorporates both individual and systemic (market size adjusted) risk factors for each criterion, and this approach may reduce sensitivity to high-risk activities conducted by smaller

46. Given the materiality of the banking sector, banks are required to submit the inherent risk questionnaire on a quarterly basis.
47. During 2025, CBA has developed similar questionnaires and methodology for risk assessment for currency exchange offices, investment funds and fund managers, and is planning to apply to these entities the same approach of risk assessment.
48. Only data on active customers is required and taken into consideration in the individual risk-based evaluation approach of CBA.

institutions. According to the Methodologies, inspection plans should also consider the level of each individual risk score, but this is left to supervisory judgement. The AT is therefore of the opinion that several tailored benchmarks for selected high-impact risk factors could be defined, to support more targeted supervisory responses, horizontal analysis and thematic reviews.

151. Furthermore, this could also give greater emphasis to the distinction between ML and TF risks indicators (or risk scores), with TF-specific factors not limited to jurisdictional breakdown of cross-border transfers or customers and high risk NPOs. Nevertheless, given the low TF risk identified in the NRA, this limitation is not considered material.

152. Following the evaluation of inherent risk, the quality of the control environment is assessed based on responses to questions included in the risk evaluation questionnaire and on scrutiny of accompanying documents, including enterprise-wide risk assessments, transaction monitoring rules and procedures, risk classification methodologies, training records, board meeting minutes, management information, and internal audit reports. A sample of client files (approximately 25 files per institution) is also required by the supervisor to test the compliance with the internal controls. Based on the information submitted, the supervisor completes a separate internal questionnaire evaluating the FI's control framework by thematic area and assigning an overall level of control effectiveness. The final residual risk, on which the on-site inspection frequency is based, is calculated as a combination of the two scores through a risk matrix.

153. At sectoral level, the CBA performs risk assessment using similar parameters, with internal controls assessed based on findings of CBA's supervisory activity. The methodology for sectoral risk assessment was last updated in March 2025[49] and the most recent comprehensive risk assessment was conducted using 2024 data (see Table 3.3). Professional judgement may be applied to adjust final sectoral scores by up to two points, which introduces a degree of flexibility.

Table 3.3. Sectoral risk categorisation matrix: residual ML/TF risks (2024)

Sector	Risk Rating	On-site inspection cycle prescribed by the institutional Methodology
Banks	high	1 to 4 years
MVTS providers	medium high	2 to 5 years
Capital markets	medium high	2 to 5 years[50]
Credit Organizations	medium low	3 to 6 years
Central Depository	medium low	-
Pawnshops	low	n.a. (will start in 2025)
Currency exchange	low	n.a. (will start in 2025)
Insurance companies and intermediaries / credit bureau	very low	n.a.

154. The outcomes of sectorial risk assessment were primarily intended to determine inspection cycles for different FIs. Higher risk sectors are subject to shorter maximum inspection cycles. For banks, which are assessed as high risk and are the most material sector, additional scrutiny is applied through quarterly data submissions for inherent risk calculation. This demonstrates a generally risk-sensitive allocation of supervisory resources.

155. The CBA's understanding of risks is further informed by supervisory engagement and strategic analyses from the FMC. The FMC has conducted several thematic studies on cross border transfers, cash-based transactions, the effectiveness of Money Laundering Reporting Officers (MLROs) in banks, and compliance with obligations related to money transfers by FIs and has forwarded the final results

49. Decision No. 1/50L of 14 February 2023 (amended 13 March 2025) of the Chairman of the CBA, and Decision No. 1/663L of 29 December 2023 (amended 13 March 2025) of the Chairman of the CBA
50. For investment companies.

to the CBA for their perusal. As a result, the CBA has conducted its own thematic or ad-hoc inspections, including on loan acquisition process in credit organizations and EDD compliance in banks. In practice, the overall high volume of data received permits the CBA to perform horizontal analysis of critical elements, such as the 2024 banking-sector review of ML/TF risk appetite, which resulted in the issuance of targeted supervisory guidance (Risk Appetite Guidance).

156. However, the CBA's understanding of group-wide risks remained limited throughout the assessment period. The specific group risk assessment methodology relies on supervisory judgement and is dedicated to prudential and conduct elements, supplemented by analysis of intragroup transactions. Following the risk analysis conducted, all seven financial groups operating in Armenia[51] are currently assessed as low risk. Apart from this analysis, FIs are required to submit all procedures and controls to the CBA as part of the annual review process (including those at group level that were applicable to them), with recommendations to eliminate any identified deficiencies through the annual "Dear CEO" letters.

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

157. Armenian authorities have undertaken extensive outreach to strengthen FIs' understanding of ML/TF risks and AML/CFT obligations. Communication combines individualised feedback and sector-wide guidance.

158. For banks, credit organisation, investment firms and MVTS providers the CBA issues annual "Dear CEO letters", highlighting deficiencies identified during off-site annual reviews, together with instructions and deadlines for remedial actions. These letters also incorporate the FMC's assessment of the quality of STRs submitted by each bank. Follow-up meetings with bank management are held to ensure supervisory expectations are clearly understood.

159. The CBA also ensures public access to information through a dedicated AML/CFT section on its website (shared with FMC) which provides relevant legislation, guidance materials, FAQs, and analytical material. Guidance has been issued on a wide range of topics, including BO identification, indicators of suspicious activity, and typologies of fraud and pyramid schemes. Recent updates include typologies on laundering the proceeds of crime through virtual assets, and guidance on risk appetite developed following reviews conducted in 2024.

160. The CBA provides lists of domestic PEPs positions on its website, which especially smaller FIs met by the AT confirmed using regularly, and has delivered several training activities on supervisory findings and the results of the NRA.

161. The FMC complements the CBA's outreach through analytical assignments aimed at improving the operational understanding of ML/TF risks. In coordination with the CBA, the FMC has issued numerous assignments between 2020 and 2025, directed mainly at banks, MVTS providers, credit organisations, and investment firms.

162. These assignments have addressed specific risk areas, such as cross-border transactions, enhanced due diligence for cash operations, internal monitoring unit independence, and recognition and reporting of suspicious transactions. Broader thematic exercises have also been undertaken on the strategic analysis of ML/TF and proliferation-financing risks and on PEP risk management. Additionally, the FMC developed an online training platform that provides self-learning modules and resources to strengthen compliance capacity across the sector.

51. In case of international groups, CBA is never the parent supervisor (there are no foreign branches of Armenian FIs)

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

163. The level of understanding of ML/TF risks among FIs varies significantly by sector, size and complexity. Overall, banks demonstrate the most advanced understanding of how ML/TF risks materialise in their operations, while smaller regulated FIs, such as currency exchanges, exhibit a more basic and often generic appreciation of risks.

164. All FIs are required to conduct annual enterprise-wide risk assessments (EWRAs) proportionate to their size and activity, which are reviewed by CBA as part of the offsite inspections. Supervisory feedback since 2020 indicates notable improvement in the EWRA's quality, structure, and analytical depth, particularly in the banking sector, resulting in more effective risk identification and mitigation frameworks.

165. Banks and major NBFI integrate customer, product, delivery-channel, and geographic elements into their EWRAs. By 2024, all banks had developed and board-approved EWRAs that comply with the CBA's methodological requirements. These assessments combine quantitative data, such as customer profiles (including PEPs, NGOs, and clients with complex ownership structures), the volume and nature of cross-border transactions, and types of products and delivery channels—with qualitative analysis of business activities and internal controls. The data used largely mirrors that reported to the CBA through annual supervisory questionnaires and is complemented by information and typologies circulated by the FMC.

166. This integration of data-driven and judgement-based analysis has improved the consistency and comparability of inherent-risk assessments across the banking sector. Banks and larger NBFIs generally use automated systems to calculate and update risk scores on an ongoing basis, with adjustments triggered by material changes in customer profiles or transaction behaviour. The underlying risk-scoring methodologies—covering both risk criteria and assigned weightings—are typically reviewed and recalibrated on an annual basis to ensure continued relevance and alignment with evolving risk exposure and regulatory expectations.

167. Among other NBFIs, which generally exhibit lower ML/TF exposure and limited systemic relevance, EWRA frameworks are correspondingly less sophisticated but broadly proportionate to their risk profiles. Supervisory reviews indicate an improving understanding of ML/TF risks among several NBFIs, as reflected in the quality of EWRAs submitted to the CBA. Smaller securities market participants and MVTS providers tend to focus on compliance with national AML/CFT legislation, regulatory guidance, and supervisory instructions, which is commensurate with their limited operational scale and risk exposure. In this context, the absence of highly complex EWRA models does not indicate a deficiency, although the extent to which EWRA outputs are used to refine internal controls remains more developed in larger and higher-risk institutions.

168. However, the practical application of FIs' understanding of ML/TF risks into operational business management has been progressively strengthened and more thoroughly embedded in the latter part of the assessment period. A thematic review conducted in the banking sector in 2024 identified weaknesses in both the quantitative and qualitative indicators used to define banks' risk appetite frameworks. Most banks lacked a comprehensive set of quantitative indicators covering all key ML risk components (customers, geography and products), while the use of risk-limiting thresholds, such as caps on the proportion of high-risk customers within the overall customer base, remained limited. In response, the CBA issued targeted guidance to strengthen banks' risk appetite frameworks and enhance the operational integration of risk assessment. Follow-up reviews confirmed that improvements are under way, with a measurable strengthening of banks' risk models observed by mid-2025.

169. Banks met onsite demonstrated a comparatively good understanding of ML/TF risks and were able to articulate the threats most relevant to their operations. The NRA findings are well known and

broadly accepted across the sector. Banks identified the highest risk as relating to remote onboarding and different types of high-risk customers, particularly PEPs.

170. Banks' customer bases are predominantly domestic and largely retail focused. Several banks reported adopting a more conservative risk appetite, including frequent refusal of high-risk customers and even de-risking certain segments[52], which they perceive as reducing their exposure to ML/TF risk.

171. Smaller FIs, such as credit organisations, MVTS providers, and investment companies, generally demonstrate a less developed understanding of ML/TF risks. These institutions tend to describe broader national threats such as corruption, drug trafficking or tax evasion, with limited ability to articulate how such risks materialize in their specific business context.

172. During onsite discussions, most FIs demonstrated familiarity with customer risk classification and FMC-issued typologies. Larger FIs have incorporated these typologies into internal monitoring scenarios, and most institutions tailor parameters, such as thresholds, transaction limits, customers factors, to their specific business models and risk profiles. However, only some institutions develop additional risk typologies beyond those prescribed by authorities. This reliance on externally set typologies and standard scenarios, while helpful for sectoral consistency, can result in limited capacity to detect and manage new and emerging risks specific to the institution.

173. Across all sectors, the distinction between ML and TF risks remains weak. Most FIs consider TF risk to be low, reflecting the NRA conclusions, and do not identify substantive TF threats within their operations. Consequently, TF is often treated as a subset of ML risk and dedicated TF analysis, indicators or monitoring scenarios are rarely developed. Supervisory reviews confirm that while banks and several major NBFIs identify customers or transactions connected to higher-risk jurisdictions, few institutions have designed monitoring scenarios or controls specifically targeting the misuse of financial channels for TF purposes.

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

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

174. Most FIs have internal controls in place for implementation of preventative AML/CFT measures, although the complexity and robustness of these controls vary significantly depending on the materiality of the financial sectors and the size of individual FIs.

175. Larger FIs met by the AT, particularly banks and group-affiliated institutions, benefit from comprehensive CDD and transaction monitoring systems, including for remote onboarding, supported by automated alerts and escalation mechanisms, including the ability to halt transactions. These institutions generally have well-established processes for customer and BO identification, verification and record keeping.

176. The BO Registry is used mainly as a verification tool to corroborate BO information obtained through institutions' own due diligence. Several FIs noted limitations in the accuracy and completeness of registry information and therefore rely primarily on internal CDD analysis, based on documents provided by clients or obtained from external sources, with registry checks serving as a supplementary source.

177. Based on the statistics provided, inability to properly identify the BO, including doubts concerning the authenticity or completeness of supporting documents, remains one of the main

52 Some banks have mentioned not onboarding clients from certain jurisdictions considered high risk.

situations that triggers internal alerts in banks, with the situation confirmed by the representatives met onsite.

178. Apart from this, the bulk of main deficiencies related to improper application of EDD, BO identification, and STR related obligations[53], particularly the lack of proper documentation of analysis for cases that did not result in submission of reports. This overview was supported by the cases presented to the AT, covering the entire assessment period.

179. Smaller FIs apply more simplified CDD measures and post transaction monitoring procedures, often developed internally and commensurate with their narrower product range and customer base. Given the bank-centered nature of Armenia's financial sector, these institutions frequently consider the requirement of holding a bank account in order to become a customer as an important mitigating factor. While this requirement enhances the overall effectiveness of preventive measures, the AT considers that the supervisor needs to devote particular attention to how this is understood in practice, to ensure it does not translate into over-reliance on banks' CDD measures, which may undermine smaller FIs' own efforts to apply proper AML/CFT controls.

3.4.2. Enhanced or specific measures

180. FIs met onsite demonstrated a sound understanding of enhanced and specific measures and were able to explain how these are applied in practice. All institutions showed awareness of geographical risk factors, particularly in relation to high-risk jurisdictions, and described mitigation measures including EDD applied to clients, BOs and transactions linked to such countries.

181. PEP screening is carried out across all sectors. Banks and larger FIs rely extensively on commercial screening solutions, particularly for identifying foreign PEPs. During the latter part of the assessment period, due to geopolitical reasons, almost all banks underwent two thematic reviews of their screening systems (in 2023 and 2024). The first round identified deficiencies primarily operational in nature, including gaps in maintaining historical records of listings and de-listings, incomplete audit trails for match resolution, shortcomings in periodic testing, and insufficient documentation of system recalibrations. The second round confirmed that most of these deficiencies had been corrected. However, recent inspections still identify instances where automated screening outputs were not sufficiently complemented by additional verification or contextual analysis.

182. Smaller FIs, reflecting their predominantly domestic customer base and the particularities of their products focus predominantly on identifying domestic PEPs. Across sectors, a recurrent deficiency concerns the identification of PEP-associated persons, with most institutions considering only family members as associates of PEPs. This limited understanding can result in gaps in identifying true associates and associated risks, leading to potential vulnerabilities in the system, especially as the majority of, if not all, cases of ML derived from corruption presented to the AT, include the use of different types of associates outside the PEP's family members (driver, former classmate, or close acquaintances).

183. Based on the cases presented to the AT, weaknesses were identified in the application of EDD measures, particularly in situations involving higher-risk customers and complex ownership structures. In these cases, deficiencies in the depth of enhanced scrutiny limited institutions' ability to fully assess customer risk and detect potentially suspicious activity.

184. Technology-related risks primarily arise from reliance on third-party screening solutions (for sanctions, PEPs and adverse media), and from non-face-to-face onboarding processes. While larger FIs,

[53] This information is also included in the official annual reports of FMC, where BO identification, EDD application and STR submission are the areas where deficiencies have been recurring in the review period.

particularly banks, regularly test and calibrate these tools and technologies, their use and validation remain less developed among smaller FIs.

3.4.3. AML/CFT reporting obligations, tipping off

185. While the authorities indicated that extensive outreach and feedback have contributed to improvements in the quality of STRs, particularly in terms of analytical content and clarity, the AT considers that the overall level of reporting across the financial sector has remained modest throughout the assessment period (see Table 6.1).

186. This observation is particularly relevant for the banking sector, which represents the most material segment of the financial system. Data broken down by individual institutions shows no clear upward trend in STR reporting, with volumes varying considerably from year to year across banks. This pattern appears inconsistent with the rapid expansion of the financial sector, which has experienced substantial growth in total assets, as well as in the number of customers and the volume of transactions processed. A similar dynamic is observed among other types of FIs, notably MVTS providers and investment companies, where STR reporting levels have remained limited throughout the assessment period, despite their risk exposure and the rapid increase in their activities in recent years.

187. The explanation provided by the authorities, that some STRs are counted as one, even when multiple notifications are received, involving several clients in relation to the same scheme, can only partly explain this pattern. While this may account for some instances, the overall evolution of reporting is not commensurate with the expansion of the financial sector and the evolving risks presented by the country.

188. During on-site discussions, many FIs described a low-risk appetite both at onboarding and during ongoing monitoring, with a tendency to decline high-risk customers or products. At the same time, the AT observed a degree of reluctance to submit STRs in situations involving doubts about the legality of customers or transactions. Instead, institutions frequently relied on customer rejection, transaction refusal, or termination of business relationships as sufficient mitigating measures, without also filing an STR. While such actions can reduce immediate exposure, this practice limits the flow of actionable financial intelligence to the FMC and, in certain circumstances, may risk alerting customers to underlying concerns, potentially affecting future detection or investigative efforts.

189. Most of the inspections triggered by intelligence from the FMC included cases of evident suspicious activity that was either not identified, documented or not reported by the FI.

3.4.4. Internal controls, procedures and audit to ensure compliance

190. All FIs met onsite confirmed that they have internal procedures and monitoring units in place to ensure effective ML/TF risk management. For the few FIs that are part of international financial groups, internal procedures are adapted to meet Armenian legal requirements while following group-level guidelines.

191. Larger FIs typically engage external auditors to test the effectiveness of their internal controls and systems, while smaller FIs rely on internal audit functions. The CBA has conducted reviews to evaluate monitoring systems of banks and larger FIs. These reviews indicate that larger FIs broadly align with international best practices, whereas smaller FIs continue to apply more limited and less risk-sensitive internal control frameworks.

192. During the review period, the CBA introduced qualification requirements for internal monitoring units in banks, mandating that the head and at least half of staff hold internationally recognized qualifications, which has strengthened institutional capacity in the banking sector. In line

with the sectoral ML/TF risk assessment, this obligation is currently applied to banks as the most material and higher-risk segment, while similar requirements are not mandated for smaller FIs.

193. Notwithstanding improvements in institutional frameworks, a recent on-site inspection identified one case in which deficiencies in the application of EDD measures resulted not from limited understanding, but from the voluntary non-application of internal rules by certain managers and staff. While this appears to be an isolated instance, it nevertheless highlights vulnerabilities in internal enforcement mechanisms and the importance of sustained supervisory engagement to support effective compliance culture. Following the internal investigation, the FI terminated the employment contracts of the employees involved.

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

194. Until recent amendments to the AML/CFT Law (July 2025), the definition of financial groups covered only banks, investment companies, insurance companies and intermediaries, and the Central Depository. As a result, MVTS providers and other FIs faced limitations in sharing AML/CFT related data within group structures, as confirmed during onsite discussions. Recent legislative changes have addressed this gap, extending information sharing obligation and thereby strengthening group-wide risk mitigation.

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

195. Until 2020, AML/CFT supervision remained integrated within broader prudential oversight. A first acknowledgement of AML/CFT specific risks came in 2017, with the adoption of CBA's Manual for Supervision for Banks and Insurance Companies, which included a dedicated section with ML/TF risks, feeding into the overall planning of supervisory actions. Since 2020, AML/CFT supervision of FIs has gradually been individualised, with the development and application of separate ML/TF risk assessment Methodologies, first for banks, and two years later for other material NBFIs. In addition, in 2020, a specialised AML risk analysis unit was established within the FSLD.

196. In practice, AML/CFT inspections are now performed separately from prudential supervision, except for very small FIs such as currency exchange offices.

197. The CBA's risk-based approach to supervision is multi-pronged. First, at sectoral level, greater supervisory consideration is given to banks, due to their materiality and overall higher level of ML/TF risk. This translates into more detailed oversight, compared to other FIs. Second, the CBA uses thematic inspections to assess compliance of an entire sector or population in a specific area. Almost all banks have undergone scrutiny of their TF/PF monitoring systems and their level of compliance with transfer of funds regulations, twice during the last two years of the assessment period. Also, in 2024, banks' engagement with VASPs was analysed and one bank with the highest exposure was selected for a targeted on-site inspection.

198. Third, at individual level, more in-depth and more frequent on-site inspections are envisaged for those FIs that show higher ML/TF risk scores. However, the rule for cyclical on-site inspections, which prescribes their frequency based on the overall risk of individual FIs, was introduced in practice starting in 2024 (with official adoption in 2025). Up to the end of the assessment period, two such on-site inspections had been finalised in the banking sector, with one under way, while five such cyclical on-site inspections have been performed in the non-banking financial sector. Recent inspection reports of this new approach reviewed by the AT, indicated a high level of comprehensiveness, covering CDD, transaction monitoring systems, correspondent banking relationships, and STR reporting.

199. As a consequence, during most of the assessment period, AML/CFT supervision relied primarily on off-site monitoring tools, and on inspections performed mostly in response to external triggers.

200. Off-site reviews are based on the annual questionnaires for risk assessment that also include supporting documentation enabling the CBA to develop a broad understanding of compliance practices of FIs included in the process.[54] This supervisory element of the questionnaires is complemented by off-site sampling of client files, that the CBA choses usually from the list of high-risk customers provided by the FI. Following the annual analysis, the CBA issues individual “Dear CEO” letters to material FIs, highlighting deficiencies identified along with recommended remedial actions and deadlines for correction. Higher risk FIs receive more detailed letters and recommendations.

201. Therefore, up until the introduction of full-scope on-site inspection cycles in 2024/2025, this off-site framework had been the central supervisory tool for AML/CFT risk-based supervision during most of the assessment period. The AT acknowledges that the off-site tool effectively captures a comprehensive view of the activities of each FI, superior to a simple supervisory questionnaire, through the fact that it entails a review of all internal documents and sampling of files. At the same time, the AT cannot consider this to be a full substitute for a risk-based supervisory approach. All institutions of a given type are subject to identical general information requests regardless of their individual risk profiles, and the off-site sampling of client files appears limited. Identified deficiencies are included in “Dear CEO” letters with recommendations for improvement which, although followed up upon by the CBA, are not to be considered enforcement measures. Conversely, the findings from the recent risk-based round of on-site full scope on-site inspections, which resulted in some of the highest sanctions of the last five years, indicate a relatively large number of serious breaches that had not been discovered before.

202. In practice, until the latter part of the review period, supervisory inspections, whether on-site or off-site, were mostly triggered by intelligence received and case referrals from third parties (particularly the FMC), targeting specific elements, such as the application of EDD for certain customers part of investigations, or verifying how the FIs had applied monitoring orders given by the CBA in regard to certain clients. A number of cases where inspections had been initiated due to internal triggers, such as a rise in activity or in the client base, were presented to the AT. This demonstrates that individual elements of the risk methodology are taken into consideration, but stronger and more formal use could be developed.

203. Cooperation between the CBA and FMC is close and institutionalised, supported by shared premises and a cooperation manual covering joint planning, information exchange, coordinated supervisory actions (including joint inspection teams), and training. Over 40 cases of potential AML/CFT breaches were referred by the FMC to the CBA during the assessment period for supervisory follow-up. Through its access to the bank account registry and customer-level data, the FMC identifies higher-risk cases and emerging compliance concerns, requests customer files from FIs, and transmits targeted findings to the CBA. This cooperation significantly informs supervisory prioritisation and enables earlier detection of compliance weaknesses.

204. While this mechanism effectively captures emerging risks, it remains predominantly reactive, concentrating supervisory efforts on FIs where risks have already materialised, and does not fully substitute for a proactive, preventive supervisory planning. As a consequence, in the banking sector alone, seven out of 18 banks had not been inspected during the assessment period outside of the annual off-site monitoring tool and the thematic inspections on TF/PF and compliance with transfer of funds regulations, although their risk level was situated in the upper part of the scale.

[54] Banks, investment companies, MVTS providers, credit organisations and Central Depository.

Table 3.4. On-site and off-site examinations (2020-mid 26.09.2025)

Sector	01.01.2020 – 31.05.2024				01.06.2024 – 26.09.2025			
	on-site		off-site		on-site		off-site	
	Full scope	Thematic /Ad-hoc	Full scope	Thematic /Ad-hoc	Full scope	Thematic /Ad-hoc	Full scope	Thematic /Ad-hoc
Banks	0	20	69[55]	38	3	34	35	17
MVTS providers	0	0	11	17	3	6	21	14
Investment Firms	0	1	12	27	2	0	35	0
Credit Organizations	0	4	0	19	0	0	77	3
Currency exchange offices	0	39	0	34	0	0	1	21
Pawnshops	1	0	0	0	0	0	0	0

205. Since mid-2024, there has been a marked increase in on-site supervisory activity, largely due to thematic inspections and the operationalisation of the risk-based cyclical framework.

Box 3.2. Case Study – Supervisory action informed by risk analysis and intelligence

Case 1: Following identification by the FMC of weaknesses in EDD practices across several banks, the CBA conducted targeted follow-up inspections, confirmed the deficiencies, and applied escalating corrective measures, including fines, orders to strengthen internal control functions, and, in one case, removal of the MLRO. These actions demonstrate the CBA's capacity to deploy a graduated supervisory response where significant compliance failures are identified.

Case 2: In early 2022, based on prudential data and intelligence from the FMC indicating sharp increases in currency exchange transactions, the CBA together with FMC conducted joint on-site inspections in five banks. These inspections identified deficiencies in customer risk classification, application of CDD/EDD measures, and transaction monitoring. All banks were issued formal remediation orders, accompanied by proportionate monetary sanctions

Source: FMC

206. Smaller FIs are supervised through a more general approach by the CBA, although a methodology for risk assessment of currency exchange and pawnshops was also adopted in 2025, which should guide the supervisory response. Supervision for these entities also takes into account data related to their activity sent to the CBA or FMC (TTRs, general activity reports) and considers their particular characteristics. For example, in the case of currency exchange offices, mystery shopping is often used, as confirmed by the entities met by the AT, to check compliance with legal obligations. Video recordings are also mandatory and can be reviewed by the CBA. Entities met on-site pointed out that CBA's inspections have become more rigorous in recent years.

207. While, technically, non-public investment funds were not under the CBA's supervision due to lack of a proper legal framework, this shortcoming was partially addressed in 2018 when the CBA requested such entities to send quarterly reports, including information about their clients, and requested that all investments be channelled through bank accounts, thus indirectly covering CDD requirements. Although this allowed for some oversight, it cannot be considered sufficient to prevent misconduct. Though the materiality of such funds has been considered as relatively low, their activity has shown a sharp increase since 2023, with a total amount of investment of around EUR 350 million, similar to other financial subsectors. This vulnerability was considered in the most recent sectoral risk assessment (2024).

55 The number of off-site full scope inspections is represented by the number of questionnaires sent by the FIs and analysed by the CBA; therefore, their number is relatively constant through the years, and it is equal to the number of FIs targeted.

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

208. Overall, the CBA's supervisory activity has had a positive and measurable impact on the compliance behaviour of FIs, particularly banks, where repeated supervisory engagement, remedial measures and sanctions have led to improvements in internal controls, staff expertise, and reporting quality.

209. The CBA systematically monitors the implementation of remedial measures imposed on FIs and conducts follow-up actions or sanctions where non-compliance persists. The authorities provided several examples illustrating how supervisory interventions have led to improvements in AML/CFT compliance. One important tool is the review of internal controls in FIs as part of the annual risk assessment, which leads to "Dear CEO" letters highlighting deficiencies. Although these findings usually do not translate into sanctions, their proper remediation is followed up by the CBA.

210. One case arose from an FMC-led analysis. Following identification of weaknesses in CDD practices across several banks, the CBA conducted follow-up inspections, confirmed the deficiencies, and imposed a series of escalating sanctions to ensure full remediation (see Table 3.5). These included fines, orders to strengthen internal monitoring units, and ultimately the removal of non-compliant MLRO. The sequence of progressively applied sanctions demonstrated the CBA's readiness to enforce corrective action until compliance was achieved (see Table 3.5). Banks concerned acknowledged that resource limitations had initially constrained implementation but subsequently enhanced their compliance capacity.

Table 3.5. Escalating sanctions implementation example

Entity	Inspection 2021 (sanctions applied)	Follow-up 1 2022 (sanctions applied)	Follow-up 2 2023 (sanctions applied)	Follow-up 3 2023
Bank 1	fine (EUR 5 000)	Fine (EUR 10 000)	✓	n/a
Bank 2	fine (EUR 25 000)	Fine (EUR 15 000)	Fine (EUR 40 000)	✓
			Fine against MLRO (EUR 2 500)	
Bank 3	fine (EUR 75 000)	Fine (EUR 150 000)	Fine (EUR 220 000)	✓
		Fine against MLRO (EUR 2 300)	Removal of MLRO	
			Limitation of activities with high-risk clients	

211. The case also triggered sector-wide remedial measures, notably the CBA's 2022 decision requiring all banks to strengthen their internal monitoring units and ensure that the MLRO and at least half of compliance staff obtain internationally recognised AML/CFT qualifications. As a result, the number of AML/CFT staff within banks increased from 82 in 2021 to 148 in 2024, with over 100 certified officers. The AT considers these developments as a key factor contributing to the improved risk understanding and compliance culture observed in the banking sector.

212. Although the content and analytical quality of STR reports have improved, particularly within the banking sector, overall STR volumes remained modest throughout the review period.

213. As mentioned above, in 2024, the CBA required all banks to document their risk appetite and introduce quantitative indicators within their internal risk assessment frameworks. An interim follow-up concluded that some of the banks have fully complied while others are in the process of implementation. These measures are expected to strengthen the alignment between business risk assessment and operational controls.

214. The CBA's sanctions framework complements its remedial measures. The supervisor is empowered to impose a full range of sanctions and has increasingly used them in recent years. Statistics provided indicate growing enforcement activity, with the banking and currency exchange sectors accounting for the majority of actions (see Table 3.6). This increase has been particularly observed in the latter part of the assessment period, mirroring the expansion of on-site supervisory activity and in line with the rapid expansion of the financial sector.

215. Of the approximately EUR 1.5 million in fines imposed on banks during the review period, around one third was applied in the third quarter of 2025 alone, reflecting not only the increase in the sector, but also a more assertive enforcement stance in response to identified compliance deficiencies.

216. An increase in sanctioning followed the application of the cyclical on-site inspections prescribed in the Methodology, which demonstrated greater effectiveness of this tool in discovering and addressing breaches compared with the previous approach described in Core Issue 3.5.

Table 3.6. Sanctions applied for FIs for AML/CFT breaches (2020-Q3 2025)

Entity	Warnings	Fines				MLRO removal	License withdrawal	License suspension
		No.	Of which against MLRO	Amount (EUR)	Of which against MLRO			
Banks	38	35	4	1 485 902	9 664	1		
MVTS	5	3		7 248				
Investment companies	1						1	
Credit organizations	13	11		242 818				2
Currency exchange	53	19		130 469			2	4
Pawnshops	1							

217. While the sanctioning methodology lists factors to be considered, it does not provide for a quantitative formula for fine calculation, leaving significant discretion to the supervisor.

218. Only brief information on sanctioning is published on the CBA website, without details on the actual sanctions imposed or on deficiencies identified[56], thus having limited impact on improving transparency and or having a deterrent effect. Although fines and administrative measures are applied more frequently, the CBA continues to view license restrictions or business limitations as an effective tool. Overall, the sanctions regime appears proportionate and dissuasive. Only five decisions of the CBA have been appealed in court, suggesting that FIs generally accept the supervisory findings and remedial measures imposed.

56. The announcements on the website only refer to the fact that a FI was sanctioned, not indicating the law or cluster of legal provisions that were breached or the level of sanction applied.

Chapter 4. Non-financial Sector Supervision and Preventive Measures

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

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Higher risk DNFBPs (casinos, online gambling operators and notaries) as well as advocates have licensing or registration regimes in place, preventing criminals from entering the market, although analysis does not always specifically include the BO. Market-entry controls for other DNFBPs remained largely absent during the assessment period. resulting in limited visibility over the sector. FMC has had to identify DNFBPs through ad-hoc discovery since assuming supervisory functions in 2023, and no legal gatekeeping measures exist to prevent criminals or their associates from entering the market.

b) Since 2023, the FMC has taken significant steps in establishing an AML/CFT supervisory framework, despite very limited resources. Its efforts have progressed from identifying reporting entities and conducting awareness raising activities to collecting data, conducting risk assessments, and providing feedback with particular emphasis on higher-risk sectors such as real estate agents.

c) Supervision of the gambling sector by the SRC reflected a general understanding of ML/TF risks aligned with the NRA but lacked a structured risk-based methodology and relied largely on ad hoc triggers, such as publicly announced major winnings or tax-related information. Supervisory activity in this sector was uneven, limiting the consistency and effectiveness of oversight. Supervision of notaries by the MoJ remains limited, constrained by resources, data availability and the lack of tailored analytical tools, despite the adoption of a basic risk-assessment methodology in late 2023 and some recent increase in oversight activity.

d) The FMC's strategic analyses and its cooperation with SRC and MoJ have contributed to a broader understanding of ML/TF risks in the DNFBP sector, particularly through analytical support and coordinated training. However, these activities do not substitute for structured, ongoing AML/CFT supervision by the designated competent authorities.

e) AML/CFT supervision of advocates is absent. ChoA's oversight is limited to disciplinary proceedings and considers attorney-client privilege to preclude AML/CFT supervision. As a result, no AML/CFT inspections have been conducted in the assessment period.

f) Understanding of ML/TF risks and AML/CFT obligations varies widely across DNFBPs. The casinos and gambling operators demonstrated the strongest understanding of risks and apply relatively robust controls. Other, smaller DNFBPs have a less developed understanding of risks. With the exception of legal professionals, most had little, if any, knowledge of AML/CFT obligations before 2023, when supervisory engagement in the sector intensified.

g) Overall, the use of sanctions and remedial measures across DNFBP sectors has been limited and uneven and have not demonstrated a consistent or sufficiently dissuasive effect, with the exception of some recent enforcement action in the gambling sector. Since establishing its supervisory role, the FMC has initiated a limited number of remedial actions (primarily warnings) and has placed greater emphasis on promoting compliance through awareness-raising activities. No AML/CFT- related measures were applied to advocates, and the MoJ's disciplinary actions in relation to notaries have been modest.

Key Recommended Actions (KRA)

a) Armenia should introduce registration or licensing requirements for all DNFBPs under FMC supervision to ensure full supervisory visibility and implement effective measures to prevent criminals from entering the market. These regimes should include fit-and-proper requirements, encompassing criminal background checks and verification of BO, and the FMC should be provided with legal powers to refuse, suspend, or revoke authorisations where individuals or entities are found unfit.

b) Armenia should prioritize operationalization of the new Operating Centre and ensure continuity of AML/CFT supervision of gambling operators during the transition. The SRC should develop and implement a risk-based supervisory methodology for the gambling sector, supported by adequate tools and sector-specific data.

c) Armenia should establish effective AML/CFT supervision of advocates, including implementation of risk-based framework with inspections and dissuasive sanctions.

Other Recommended Actions

a) Armenia should increase human and technical resources for DNFBP supervision, particularly within the FMC and MoJ. The MoJ should invest in AML/CFT analytical tools to operationalize its risk-based methodology for notaries. Armenia should invest in automated tools to enable the FMC to identify newly established entities performing AML/CFT relevant activities falling under its supervision.

b) The FMC should continue strengthening its supervision, including through onsite inspections and the imposition of escalating remedial measures and sanctions in cases of repeated non-compliance.

c) Armenia should place greater emphasis on training for the DNFBP sector with enhanced focus on TF-related risks.

Overall conclusions on IO.4

Supervision of AML/CFT compliance by DNFBPs in Armenia has been applied unevenly throughout the review period, with significant variation in approach, intensity, and effectiveness across sectors and supervisory authorities.

Supervision of the gambling sector by the SRC reflected a general understanding of ML/TF risks aligned with the NRA but lacked a structured risk-based methodology and was uneven, with inspection activity discontinued for nearly two years before resuming towards the end of the review period. The MoJ conducts very limited oversight of notaries, constrained by lack of resources, though engagement increased during the latter part of the review period, primarily through outreach and training. For advocates there is no meaningful AML/CFT supervision. Since 2023, the FMC has made notable progress in establishing an AML/CFT supervisory framework for less material DNFBPs, despite highly limited resources, with particular emphasis on higher-risk sectors such as real estate agents, though implementation remains at an early stage.

The use of sanctions and remedial measures has been limited and not sufficiently dissuasive. The FMC has initiated limited remedial actions (primarily warnings) and has placed greater emphasis on promoting compliance through awareness-raising. The SRC has taken some recent enforcement action in the gambling sector, and the MoJ's disciplinary actions regarding notaries have been modest. No AML/CFT-related measures were applied to advocates.

Understanding of ML/TF risks and AML/CFT obligations varies widely across DNFBPs. Casinos and gambling operators demonstrated the strongest understanding and apply relatively robust controls, while other DNFBPs have less developed understanding. Most had little knowledge of AML/CFT obligations before 2023, when supervisory engagement intensified. Reporting of suspicious transactions remains insufficient relative to the risk profile of the sectors, highlighting the need for continued supervisory engagement, guidance and enforcement effort.

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

219. DNFBP supervision in Armenia is shared across several authorities: (i) SRC for casinos and gambling operators; (ii) MoJ for notaries; (iii) ChoA for advocates; and (iv) FMC, which is responsible for supervising real estate agents, lawyers and legal firms, accountants and DPMS.

220. Online casinos and e-gaming platforms represent the most material DNFBP sector in Armenia, in terms of risk and volumes. The AT focused in particular to e-casinos and e-gaming entities, since those account for almost 99% or the total gaming sector and have encountered a significant growth in the years.[57] Notaries, which also count for high materiality, along with real estate agents were given also particular interest, given that transfer of property was indicated by authorities as one of the prevalent methods for money laundering (see further Materiality of FIs, VASPs and DNFBPs).

221. The previous evaluation identified significant shortcomings: (i) the absence of meaningful market-entry controls for most DNFBPs; (ii) limited risk awareness among supervisors; (iii) the absence of risk-based supervision; (iv) ineffective sanctions; (v) negligible supervisory impact; and (vi) weak awareness and implementation of AML/CFT obligations by DNFBPs. While comprehensive reforms have been introduced since 2023, particularly through the establishment of FMC's supervisory unit, some of these deficiencies continue to affect the overall effectiveness of Armenia's DNFBP supervision.

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

4.1.1. Market entry controls

222. Market entry controls are applied in a more proactive manner in sectors subject to formal licensing regimes, such as casinos, notaries and advocates, where fit and proper checks are conducted systematically at entry, whereas for DNFBPs under FMC supervision, the approach was largely reactive

57. From a turnover of approximately USD 1.6 bn. in 2018 to USD 18 bn. in 2024 (source SRC)

during most of the assessment period, relying on post-hoc identification of entities and ad-hoc scrutiny in the absence of a comprehensive registration framework.

MoF – Casinos and online gambling operators

223. For casinos and gambling operators the MoF performs fit-and proper checks of qualified shareholders, BOs and managers. Screening is checklist-based, aligned with legal requirements and includes scrutiny of the criminal record. During the assessment period all fit and proper reviews involved Armenian citizens only. Scrutiny is conducted at the market entry stage and there is no proactive ongoing monitoring. Following licensing the checks would only occur upon trigger events brought to the attention of MoF.

224. The understanding of beneficial ownership is limited and refers mostly to direct or indirect shareholding, as opposed to identifying the ultimate natural persons who own or control the entity. The market is small, and the authorities confirmed that the ownership structures are not complex. Accordingly, although BO scrutiny is basic, the authorities maintain a general overview of the sector ownership. There are only four land-based casinos and five online gambling operators, with all except one (which is part of an international group with a listed parent company) being controlled by Armenian residents.

225. Although appointed managers may perform their duties up to three months prior to receiving the official license, authorities confirmed that in practice the scrutiny checks are conducted much faster and any adverse information would be swiftly discovered. One example was provided to the AT of a CEO application rejected due to adverse information related to family-related bankruptcy proceedings.

MoJ – Notaries

226. The MoJ is the licensing authority for notaries. As notaries operate only as sole practitioners, all market-entry scrutiny focuses on the applicant. The licensing process is comprehensive and includes evaluation of both professional competence and reputation, through formal examinations and document checks.

227. Criminal record checks are carried out through formal requests to the MoI, with responses received directly in hard copy. Where necessary, additional information can be requested from other competent authorities, such as the NSS, although this is done on an ad-hoc basis.

228. Eligibility for appointment as notary is restricted to Armenian citizens. While no applications have been received from individuals with foreign residency, the authorities indicated that, in such cases, criminal record information would be requested from the relevant foreign jurisdiction.

229. Ongoing monitoring is covered by legal provisions requiring notification to the MoJ whenever a criminal proceeding is initiated against a notary. No such cases occurred in the assessment period.

FMC (*real estate agents, lawyers and legal firms, accountants, DPMS*)

230. For most of the assessment period, real estate agents, lawyers, accountants and DMPS providers were not subject to any registration or licensing requirements, meaning there was no effective market entry controls to prevent individuals or entities with criminal connections from operating in these sectors.

231. Following recent legislative changes, these DNFBPs are now required to register with the FMC. Given the availability of data in its own databases, FMC performs scrutiny on market participants, albeit there is no regulatory requirement for this and no legal powers to reject individuals if adverse data is identified. Upon assuming this role in 2023, and in the absence of automated verification tools or systematic triggers to identify entities falling within the scope of the AML/CFT framework, the FMC prioritised mapping the sector and determining which entities were required to register. To this end, the

FMC relied on a range of ad-hoc measures, including targeted questionnaires, analysis of open-source and economic classification data (activity codes in the companies register), as well as reviews of available bank account data[58]. These measures constituted a one-off identification and entry-screening exercise for the newly regulated DNFBPs**.** To address the absence of automated detection mechanisms, a protocol is envisaged to introduce a dedicated trigger in the SRC system to flag companies whose activities indicate that they qualify as reporting entities under AML/CFT Law.

232. Fit and proper checks rely on open-source data, information received from banks, and intelligence available to the FMC in its capacity as the FIU. Given the predominantly local nature of the DNFBPs concerned and their generally simple ownership structures, this approach has been largely adequate to identity integrity concerns at the market entry-stage in straightforward cases. No adverse information was discovered through these checks, except in one case of a real estate agent colluding with a criminal. The matter was referred to LEAs and the manager was subsequently dismissed by the company.

233. However, the scope and preventative effect of these controls remain limited. There is no legal or regulatory fit-and-proper regime (no requirement for criminal checks) covering owners, BOs, controllers, or managers of DNFBPs supervised by the FMC. Any screening undertaken by the FMC is policy-based and non-binding, and the FMC lacks statutory powers to refuse, suspend, revoke, or otherwise restrict a DNFBP's business on fitness grounds. Consequently, there is no mechanism to systematically prevent criminals or their associates from holding significant or controlling interests or exercising management functions in FMC-supervised DNFBPs.

ChoA - advocates

234. Criminality checks are performed for individuals applying to become advocates. Candidates are required to submit a criminal record certificate, although the ChoA is also empowered to request such information directly from the MoI. However, there are no effective mechanisms to verify criminal records issued outside Armenia, which limits the robustness of checks in cases involving foreign residency or prior activity abroad.

235. Given the relatively strict eligibility criteria for entering the profession, the ChoA reported that no cases of individuals with criminal convictions attempting to obtain an accreditation were identified during the assessment period. The AT was nevertheless presented with one case in which a candidate failed to provide the required criminal record certificate and was rejected at an early stage of the application process. This example demonstrates that basic integrity checks are applied in practice, although they remain largely document based.

236. In terms of ongoing controls, the ChoA reported two cases in 2025 where an advocate's license was terminated. In one case, the termination followed automatically from a final court decision against the advocate. In the second case, the disciplinary committee revoked the license due to public statements of the advocate deemed incompatible with the professional and ethical requirements of the profession.

4.1.2. Detecting and addressing breaches

237. In the gambling sector, there is no regular post-licensing monitoring and detection of breaches relies on specific triggers or external information. Nevertheless, mechanisms exist to address unlicensed activity: the SCR monitors online gambling activity and refers unlicensed websites to the competent authority for blocking, resulting in approximately 1 000 websites being blocked during the assessment period, while cases of unlicensed land-based gambling would be referred to LEAs (no such breaches identified in the assessment period). For notaries and advocates, ongoing controls are limited to event-

[58]. FMC has the power to request data from banks in its FIU capacity and communicates directly with the bank's internal monitoring unit through the CBA.net system.

driven mechanisms, such as mandatory notifications following criminal proceedings or final court decisions, rather than systematic periodic reviews. By contrast, for DNFBPs supervised by the FMC, detection of unregistered or unauthorised activity has been limited, reflecting the absence of systematic monitoring tools and the recent introduction of registration requirements. Overall, with the partial exception of online gambling, the approach to detecting and addressing breaches across DNFBPs remains predominantly reactive.

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

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

238. Overall, supervisors' risk understanding in the DNFBP sector is closely tied to the NRA process. For each NRA exercise, supervisory authorities perform their own sectoral analysis and submit the result and underlaying data to the FMC for inclusion into the final report. This analysis forms the basis of the sectoral risk assessment, as no other standalone assessments or alternative methodologies are used to evaluate ML/TF risk at the sectoral level. Therefore, supervisors also reference the findings of the NRA when articulating the risks to which their sectors are exposed.

SRC – Casinos and online gambling operators

239. The SRC's understanding of ML/TF risks in the gambling sector broadly reflects the NRA findings, with internet gambling assessed as presenting the highest risk. However, the SRC does not have developed a dedicated AML/CFT risk-assessment methodology, and its risk analysis relies mainly on the tax-related data and information on large winnings published on the official websites.

240. Despite these limitations, the SRC demonstrated awareness of key sectoral threats and typologies. During the assessment period, several mitigating measures were introduced, including a requirement that all top-ups and pay-outs to be made through the same bank account held in the player's name (October 2024), which contributes to mitigating anonymity and misuse risks.

241. TF risk in the gambling sector is considered low, reflecting legal requirements for all online gambling players, resident and non-residents, to use accounts with Armenian banks, as well as declining number of non-resident players. This assessment is consistent with the NRA and was supported by information provided to the AT.

MoJ – notaries

242. The main activity of notaries relevant under FATF Methodology is the notarization) of real estate transactions[59]. While some information was provided to the AT on the existence of notaries that also engage in activities specified by R.22, let. d) points (iv) and (v), the MoJ could not confirm this aspect.

243. In late 2023, the MoJ adopted a methodology requiring an annual AML/CFT risk-assessment of notaries. The methodology categorises notaries into low, medium and high risk based on a limited set of predefined criteria, such as involvement of PEPs or parties linked to higher-risk jurisdictions. However, the framework remains basic and does not incorporate a broader range of risk indicators or criteria.[60]

244. In practice, the MoJ currently lacks the data necessary to apply this methodology effectively. Although notaries submit quarterly reports on transaction volumes, no systemic data is collected on the

[59] In Armenia, only transactions that involve real estate above AMD 50 million (approx. EUR 100 000) and donations have to be notarized.

[60] Although the Methodology makes reference to quantitative criteria, it is not clear how this should be considered.

identity or characteristics of parties to transactions. As a result, the MoJ's understanding of risks in the notarial sector remains largely based on aggregate transaction volumes and complaints received. Authorities have indicated that a new IT system is to be introduced, which would enable access to more granular data and support fuller implementation of the risk-assessment model.

FMC - (*real estate agents, lawyers and legal firms, accountants, DPMS*)

245. Since assuming AML/CFT supervisory responsibilities in 2023, the FMC has taken initial steps to develop a risk-based understanding of ML/TF risks across the sectors it supervises. At sectoral level, the understanding of risk derives from the NRA findings, which point real estate agents as relatively higher risk entities among those supervised by the FMC. At individual level, the risk assessment methodology is prescribed in a Supervisory Manual and is based on structured questionnaires sent to reporting entities, collecting information on inherent risk factors (customers, services, delivery channels, geographic exposure) and on internal controls. The outcome is based on scores from 1 to 3 attributed to each criterion, which feed into a matrix[61], providing a segmentation of DNFBPs into three final categories of residual risk: low, medium and high. In total, there are over 20 criteria for inherent risk and over 30 for internal control assessment. A significant proportion of criteria are assessed by supervisory judgement, including conclusions drawn upon interactions with DNFBP personnel at different training events, and calculated manually, thus offering the FMC a high level of flexibility in determining the final score.

246. This new approach has been officially introduced in the beginning of 2025, with one round of complete risk assessment guided by the Manual. Before that, FMC has piloted the questionnaires, with analysis based on requests of data covering 2021-2023 period.

247. The results placed the vast majority of DNFBPs (under FMC supervision) in the low-risk category, with only real estate agents having a relatively taller proportion of medium and high-risk entities in their overall population[62], which is consistent with the NRA results. Under the individual methodology risk matrix, a low-risk category is only possible in case of effective internal controls, and these, as explained by authorities, are assessed proportionately to entity size. Smaller entities may be deemed compliant with basic measures while larger entities are expected to demonstrate more robust controls. However, this approach is not fully consistent with information obtained through interviews with the private sector, which indicate persistent deficiencies in the entities' understanding of AML/CFT obligations.

248. The AT is of the opinion that this newly introduced system proved its effectiveness in setting up a structured foundation for developing an understanding of sectoral and institutional risks over time, particularly given the previously limited visibility over DNFBPs. However, there is need for further calibration and for automation, as the FMC (SASD) is highly under-resourced for the role of sustaining this process in parallel with the foreshadowed inspection activity.

249. During the assessment period, the FMC also produced several strategic analyses, including some with specific relevance to the DNFBP sector.63 Topics were selected based on emerging cases, statistical trends, and supervisory judgement. These analyses have contributed to the FMC's thematic understanding of risk.

[61] Inherent risk is weighted at 40%, while the level of adequacy of internal controls are weighted at 60%, thus reflecting its greater importance given.

[62] Out of 196 realtors that underwent the risk assessment, 11 are considered high risk, 14 are considered medium risk while 171 are considered low risk.

[63]. As mentioned under IO.3, the risk assessment activity of the FMC is not limited to the DNFBP sector.

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

250. The promotion of ML/TF risks awareness and AML/CFT obligations among DNFBPs has been largely driven by the FMC, while other sectoral supervisors have played a more limited role in awareness-raising activities.

251. Since 2023, the FMC has significantly intensified its engagement with DNFBPs and actively focused on raising awareness and improving DNFBPs' understanding of ML/TF risks and AML/CFT obligations, with particular attention to higher-risk sectors such as real estate agents. Supervisory efforts have included dedicated training sessions, ad-hoc engagement with entities identified as having insufficient knowledge, and review of internal procedures of selected entities. The FMC has also issued guidance papers and typologies, published on its website, and developed an e-learning platform accessible to all reporting entities.

252. The FMC communicated the results of the ML/TF and PF NRAs to all DNFBPs and held meetings in May 2025 to present and discuss the findings, with broad participation among medium- and high-risk entities.

253. During 2024-2025, representatives from all DNFBP categories, including notaries and gambling operators, participated in training sessions organised by the FMC with the support of the CoE and delivered by national and international experts. DNFBP representatives confirmed their attendance to the AT and indicated that the training strengthened their understanding of ML/TF risks and their statutory obligations.

254. In addition, following repeated deficiencies in the timely submission of TTRs, the MoJ issued a circular to the Chamber of Notaries in 2025 reminding members of their reporting obligations.

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

255. Most DNFBPs demonstrate a good understanding of national and sectoral ML/TF risks, as well as how these risks evolved over time, although the depth of understanding varies significantly across sectors. Online casinos and gambling operators, as most material sector, demonstrated the most advanced understanding of how their services could be abused for ML. Remote onboarding is intensively used, and operators have implemented robust systems accordingly. Customers are risk assessed (usually there are no low-risk clients) and the representatives met by the AT were able to articulate several ML scenarios they monitor through different gaming activities, including systems to detect fragmentation of transactions.

256. Notaries and legal professionals also showed awareness of the main threats in their activities, although understanding varies. Advocates generally have limited recognition of how their professional activities could be misused for ML, citing professional confidentiality and the perception that FATF-relevant services are not commonly performed.

257. Following extensive training in recent years, real estate agents demonstrated awareness of the basic ML threats to which the sector has historically been exposed. Industry representatives highlighted that the introduction of the cashless law has substantially reduced ML exposure, as property transactions must now be conducted through the banking system rather than cash. Nevertheless, they acknowledge that prior to this measure, cash transactions presented a higher ML risk.

258. Accountants met by the AT largely do not recognize ML risks in their sector, consistent with NRA findings that these entities do not perform activities falling under FATF Methodology. DPMS showed the least awareness of ML risks, perceiving their activities outside the scope of threats due to legal limits on cash transactions (cash payments above EUR 700 prohibited).

259. Across the DNFBP sectors, awareness of TF risk is generally informed by the NRA findings, which identify TF risk as low. Most DNFBPs are familiar with the NRA conclusions and with their AML/CFT obligations, including those related to TF. However, beyond sanctions screening—primarily through lists provided by the CBA or commercial vendors—there is limited evidence that DNFBPs consider TF risk in a more substantive or sector-specific manner. In particular, DNFBPs do not demonstrate how TF risks could materialise in their activities or how such risks are factored into their internal risk assessments or controls.

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

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

260. Online casinos and gambling operators demonstrate the most comprehensive application of CDD, monitoring and internal controls among DNFBPs. Significant human and especially technical resources are dedicated to compliance, supported by knowledgeable MLROs with relevant experience. Given the prevalence of remote onboarding, operators apply a range of mitigating measures to verify customer identity and keep client data accurate and up to date, including verification of social security numbers through national systems. The vast majority of customers are Armenian residents. While the systems described by the operators have been strengthen over time, supervisory testing during the assessment period has been limited, therefore, the AT cannot form a definitive conclusion on the sector's level of compliance. Moreover, the few controls that had been performed by the SRC identified issues of CDD improper application (such as not performing on-going monitoring and updating identification data).

261. Real estate agents have a basic understanding of their AML/CFT obligations. In practice, CDD typically consists of recording customer identification data and retaining copies of identification documents of the parties involved. Most customers are Armenian natural persons, with non-residents rarely involved in property transactions and legal persons only occasionally. In such cases, incorporation documents are reviewed and checks performed against national databases. Since the entry into force of the cashless law (2022), transactions are increasingly channelled through the banking system, and real estate agents' due diligence has increasingly relied on customers new obligation to open bank accounts and deposit purchase funds. In performing their own analysis, agents have, in effect, leveraged banks' CDD by requiring customers to provide the same documents submitted to the bank for account opening or transfer. Prior to this, real estate agents met by the AT reported that most transactions were conducted in cash and that CDD application was limited.

262. Law firms generally apply CDD at onboarding stage for both natural and legal persons, motivated both by AML/CFT requirements and the need to protect their professional practice.

263. For donations of real estate, notarisation has been compulsory since 2023. Sale and purchase agreements of real estate are not required to be notarised, Notaries perform CDD by identifying the parties and conducting basic checks (e.g., review of past transactions). The vast majority of clients are Armenian individuals (residents and non-residents). In the limited cases involving legal entities, ownership structures are simple and BOs are readily identifiable. Some misunderstandings persist regarding record keeping, notably the failure to retain evidence of all checks performed even when no negative information has been identified).

264. DPMS apply only basic CDD, primarily for commercial rather than AML/CFT purposes. Monitoring is limited, and scenarios such as possible structuring are not actively considered, although representatives stated that unusual transaction patterns would be captured and escalated internally.

265. Deficiencies persist in record-keeping practices. Some real estate agents retain records for periods shorter than statutory requirement, and some advocates demonstrated misunderstandings regarding the scope of documents to be retained, notably by failing to keep records of CDD analyses and checks performed. This was confirmed by the FMC during its data-gathering exercise, which revealed that several DNFBPs experienced difficulties in providing complete and timely information for the period 2021–2023.

4.4.2. Enhanced or specific measures

266. Online casinos and gambling operators met by the AT apply EDD measures for high-risk customers, and were able to give details, including on increased scrutiny of accounts and transactions performed, verification of source of funds for large deposits and additional open-source checks. Non-residents are generally considered high risk and are screened using commercial solutions. Foreign PEPs are identified through daily or periodic automated screening against multiple databases.

267. In other DNFBP sectors, the application of enhanced measures is uneven. Law firms met by the AT apply heightened caution for higher-risk clients and apart from the official domestic PEP list, some have their own blacklist and do not engage with clients that have criminal records. Real estate agents primarily rely on high-risk country lists published by the CBA. Across DNFBPs, requests for SoF are common, typically through bank statements or sale-purchase contracts.

268. Notwithstanding these measures, there is a widespread misunderstanding across DNFBPs regarding the identification of PEP associates, with most entities limiting their consideration to immediate family members. While DNFBPs frequently referred to the small size of the country as facilitating identification of domestic PEPs, this does not substitute for systematic identification and application of enhanced measures.

4.4.3. AML/CFT reporting obligations, tipping off

269. STR reporting across DNFBP sector remains below the level that would be expected given the ML/TF risks attributed to certain DNFBP sectors in the NRA, such as casinos and gambling operators and real estate agents. No TF-related STRs have been filed by DNFBPs during the assessment period.

Table 4.1. STR Reporting in DNFBP sector (2020-2024)

DNFBP	2020	2021	2022	2023	2024
Casinos and gambling operators	11	1	12	4	12
Real estate agents	0	0	0	0	0
Law firms and legal practitioners	0	0	0	0	0
Notaries	1	0	0	125[64]	59
Accountants and accounting firms	0	0	0	0	0
DPMS	0	0	0	0	0
Advocates	0	0	0	1	0

270. DNFBPs are generally aware of their reporting obligations; however, reporting practices suggest that suspicion is interpreted narrowly, with STRs typically filed only once alternative explanations have been largely excluded. In practice, entities often seek to resolve concerns internally reflecting a cautious approach, with a relatively high threshold before suspicions are escalated to the

[64] The sharp increase in the number of reports send by notaries in 2023 was due to the overreporting of three notaries located within the same premises.

FIU. Several DNFBPs met by the AT, including law firms, indicated that the FMC has recently encouraged more active reporting.

271. The introduction of the cashless law in 2023 has influenced reporting patterns. Gambling operators noted that before the ban, a significant share of activity was cash-based and generated STRs linked to attempts to circumvent the banking system. Following the prohibition of cash transactions, reporting has shifted towards other indicators, such as coordinated betting behaviour, unusual wagering patterns, or the placement of large bets on highly favourable odds.

272. Advocates indicated that filling STRs is considered only in relation to potential clients (prospects) or activities falling outside the scope of professional legal representation. The sole STR example provided concerned a potential client whose declared business activity was inconsistent with information available to the reporting entity.

Table 4.2. TTR* Reporting in DNFBP sector (2020-2024)

DNFBP	2020	2021	2022	2023	2024
Casinos and gambling operators	1 720	3 007	13 249	13 890	10 013
Notaries	8 973	9 754	8 312	3 597	19 164

** obligation for notaries and casino and gambling operators to report non-cash transactions above AMD 20 million (about EUR 48 000), except for transactions of buying and selling real estate and donations, which shall be reported if concluded at an amount above AMD 50 million AMD (approximately EUR 110 000).*

273. While notaries account for noticeable increase in STR and TTR reporting during the assessment period, this development is largely linked to legislative changes introduced in November 2023, which extended reporting obligations to include donation transactions. Analysis of these reports indicates that a proportion were triggered by formal or objective criteria (such as the absence of a declared family relationship between parties), rather than by articulated suspicion. This indicates that, while awareness of reporting obligations has improved, further clarification and guidance would assist notaries in applying the suspicion-based reporting threshold in a more consistent manner.

274. Overall, the quality of STRs has increased recently, as confirmed by FIU representatives. In the gambling sector in particular, the volume and quality of STRs have improved over the past year, and reports are more comprehensive, with reporting entities frequently attaching the underlying analysis that led to submission. The quality of notaries' STRs has also improved, and the FIU has confirmed that recent STRs have supported LEAs' investigations. However, notwithstanding this positive trend, the volume and nature of reporting do not yet fully reflect the spectrum of ML/TF risks identified in national and sectoral risk assessments, particularly in sectors assessed as higher risk.

4.4.4. Internal controls, procedures and audit to ensure compliance

275. All DNFBPs that are legal entities with more than 10 employees, as well as sole entrepreneurs employing more than 10 persons, are required to maintain internal AML/CFT procedures. This requirement captures the entire gambling and casinos sector. By contrast, in case of DNFBPs supervised by FMC, only about 3% reach this threshold.

276. Larger DNFBPs, such as casinos and gambling operators, generally have stronger internal controls, which are constantly updated in line with developments in the industry, and maintain internal and external audit functions. Smaller DNFBPs have more recently benefited from a review performed by the FMC of their internal acts, which incorporated recommendations and led to the improvement of those entities' overall internal approach.

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

277. There are no significant legal or regulatory impediments to implementing AML/CFT obligations and related mitigating measures.

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

278. The risk-based supervision of DNFBPs is unevenly applied across sectors. For casinos and online gambling operators, which represent the most material sector, supervision- which was largely based on triggers and professional judgement decreased in intensity in the latter years of the assessment period.

279. Other authorities have only recently introduced basic frameworks or methodologies, and their implementation has been constrained by limited resources and data gaps, resulting in a reliance on ad-hoc judgement rather than systematic, risk-driven planning. Some sectors, such as advocates, remain outside proper AML/CFT oversight. Consequently, it has not been demonstrated that supervisory intensity and coverage are consistently aligned with ML/TF risks across DNFBP sectors.

SRC – Casinos

280. Since 2018, the SRC has been responsible for supervising casinos and gambling operators. A specialized five-person unit oversees compliance with AML/CFT requirements. Supervision does not follow a risk-based methodology and relies on supervisory judgement informed by tax submissions, mandatory reporting under gaming legislation and publicly available information. There is no specific methodology, nor tools for SRC to oversee bets or payouts for AML/CFT purposes, beyond tax data and public announcements of large winnings.

281. The number of on-site inspections with an AML/CFT component remained very limited throughout the assessment period. Between 2020-2023, an average of two such inspections were conducted annually, and none took place in 2024, a year in which the authorities indicated that their supervisory approach shifted towards intelligence focused oversight, relying on third-party information. Gambling operators met onsite confirmed limited supervisory engagement in recent years, with some indicating no direct interaction since 2022 and others reporting only off-site review of periodic submissions (such as periodic reports on cash flow, winnings, and the number of players). Prior to 2024, operators met onsite confirmed that SRC inspections included the scrutiny of AML/CFT processes, including of monitoring systems.

282. This reduced supervisory activity coincided with the adoption in 2024 of new legal and structural frameworks, including the planned establishment of an Operating Centre to oversee gambling activities through an electronic monitoring system, as well as creation of a new department with 14 positions within the SRC. These reforms represent a positive enhancement of the supervisory framework; however, they were not operational during the assessment period, and their impact could not be assessed.

283. The lack of proper supervisory tools and resources within the SRC was partially mitigated by the cooperation with the FMC, including the use of FMC strategic analysis. For example, the FMC analysed data on individuals with large winnings and transmitted the results to the SRC for implementation of appropriate measures. Gambling operators also described on-going cooperation with the FMC, including participation in round table meetings.

284. Remedial measures applied by SRC were limited for most of the assessment period. Prior to mid-2025, fines imposed for failures to conduct ongoing due diligence were modest (totalling EUR 1 850). A more substantial fine of EUR 45 000 was imposed in Q3 2025 for failures related to risk-

based customer assessment, mandatory reporting and record keeping, indicating a potential shift towards stronger enforcement.

MoJ – Notaries

285. Supervisory activity of notaries is performed by the MoJ with three active inspectors responsible for all statutory oversight, including AML/CFT. Prior to 2023, inspections with AML/CFT component were rare. One case from 2021 was presented to the AT, involving delayed TTR reporting and resulting in disciplinary measures.

286. The new supervisory methodology introduced in 2023 provides for inspections on a three-year cycle. However, due to limited resources and absence of adequate data and analytical tools, this cyclicity has not yet been implemented in practice.

287. In 2023, under the National Strategy Action Plan, the MoJ requested transaction statistics from the Chamber of Notaries on all transactions legalized by notaries during 2022-2023. Based on this data, in particular the volumes of activity, coupled with the complaints received from the public, the MoJ selected three notaries for on-site inspection. These inspections identified deficiencies mainly related to late TTR reporting, and disciplinary measures were applied (reprimand). Additional inspections were conducted following a sharp increase in donation related STRs filed in 2023. These inspections identified misunderstandings of reporting obligations and no further actions were taken.

288. Notaries submit quarterly statistical data on the transactions they have legalized through an electronic system. However, the scope of data is limited to transaction volumes, and does not include information about parties involved. While additional information is occasionally requested from the FMC, the MoJ currently lacks systems and analytical tools necessary to apply a genuinely risk-based supervisory approach. Authorities indicated that a new IT system is envisaged to address these shortcomings.

FMC

289. Although the legal basis for FMC supervision was in place since 2018, actual AML/CFT supervision activity commenced only in 2023, following the establishment of the Strategic Analysis and Supervisory Division (SASD). The unit is comprised of five people, of whom only two (together with the manager) carry out supervision activities; the remaining staff having the task of delivering strategic analysis. While strategic analysis has at times complemented supervisory work (including beyond FMC-supervised entities), this does not substitute for structured supervisory engagement.

290. Given the scope of supervised sectors and the breadth of supervisory responsibilities, FMC resourcing is assessed by the AT to be highly inadequate to support effective risk-based supervision.

291. As supervisory engagement with the sector had been largely absent prior to 2023, DNFBPs demonstrated a limited awareness of their AML/CFT obligations. In response, the newly established unit initiated a structured programme of engagement combining awareness-raising activities, systematic data collection to support institutional risk assessment, and targeted feedback on internal policies and procedures, which subsequently progressed into supervisory activities.

292. In 2025, the FMC formalized this approach and adopted a Supervisory Manual which, in addition to the risk methodology described in core issue 4.2, introduces a risk-based framework for supervision, providing for on-site inspections of high-risk DNFBPs and remote supervision for medium- and low-risk entities based. However, this new architecture has been applied for only two supervisory cycles: the first one focused on outreach and securing sector-wide compliance, with the second concentrated on assessing and identifying higher-risk entities and applying proportional oversight. While on-site monitoring has not been feasible, owing to the large number of entities and resource constrains within the FMC, the risk ratings attributed through the developed risk assessment

model translated into more intensive off-site scrutiny for those higher risk entities. This has included additional engagements with those entities, in-depth analysis of their activities and enhanced expectations for, and scrutiny of, their internal controls.

293. The AT notes the strong start of the FMC in pursuing these activities in a short period of time, combining outreach with follow up on prescribed remedial measures, despite very limited resources, and acknowledges the overall improvement in entities' level of awareness, as a first step in ensuring compliance. However, to demonstrate effectiveness, supervision requires further consolidation and fuller implementation, over an extended period to prove its robustness and usability in practice.

294. Given the relatively early stage of supervisory implementation and the relatively low materiality of the sectors under its supervision, the FMC has not prioritised the use of sanctions, instead seeking to secure compliance through collaborative engagement with reporting entities. Nevertheless, in two cases involving legal firms, enforcement proceedings were initiated due to deficiencies in internal procedures and failure to provide requested information. In one case, a warning was issued, while the other firm voluntarily rectified the violations and proceedings were closed.

ChoA

295. The ChoA performs only limited oversight of advocates, based on monitoring compliance with rules of general conduct. Supervisory activities are carried out through disciplinary proceedings, as the ChoA maintains that client-attorney privilege constraints substantive AML/CFT supervision. As a result, supervision of AML/CFT compliance is not risk-based and remains limited in scope.

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

296. Supervisory authorities provided examples of outreach activities, remedial measures and isolated enforcement actions; however, there is no systematic analysis of trends in supervisory findings and compliance outcomes across DNFBP sectors. Given that, with the exception of the gambling sector, AML/CFT oversight has only recently been applied in practice, authorities do not maintain consolidated statistics on the nature, frequency or severity of AML/CFT breaches identified during this time, nor on the impact of supervisory interventions on subsequent compliance.

297. In the gambling sector, deficiencies identified during onsite inspections primarily concerned failures to properly conduct on-going due diligence, including cases where accounts with expired identification documents remained actively used. Gambling operators have subsequently taken corrective actions, including cooperation with the e-government infrastructure agency (Ekenk LLC) to strengthen identity verification process. These measures indicate a capacity to address supervisory findings in practice.

298. Across the wider DNFBP sector, understanding of AML/CFT obligations was highly limited for most of the assessment period, reflecting the relatively recent introduction of supervisory responsibilities for the FMC. Since 2023, extensive training, outreach and guidance activities conducted by the FMC have had a positive impact, and most DNFBPs met by the AT demonstrated improved awareness of their obligations and confirmed that this was due to the recent interaction with the FMC. Nevertheless, the level of understanding remains uneven across sectors, and continued supervisory engagement and outreach are required to ensure consistent implementation in practice.

299. In the gambling sector, supervised by the SRC, enforcement action has been more visible, albeit limited, and supervisory findings indicate that identified deficiencies have been followed by remedial measures and improvements over time. By contrast, enforcement action across other DNFBP sectors has been largely absent. Since assuming its supervisory role, the FMC has applied only a small number

of remedial measures; MoJ disciplinary action in relation to notaries has been modest; and the ChoA's powers are limited to professional disciplinary measures.

300. While recent outreach activities by all authorities, in particular the FMC, appear to have improved overall understanding of DNFBPs, consistent enforcement actions to ensure compliance remain limited, including in the most material sectors.

301. The absence of consistent data, trend analysis and information on follow-up actions limits the ability to demonstrate a sustained and system-wide positive impact of supervision and sanctions on DNFBP compliance over time.

Chapter 5. Transparency and Beneficial Ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40. [65]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Following the 2015, MER Armenia has implemented further measures to prevent the misuse of legal persons, the most significant being the BO register in a three-phased approach that came to an end in 2023. The BO registration is done electronically, and the authorities adopted a sanctions framework for non-compliance with reporting requirements. The most recent amendments (in August 2025) are focussed on increasing transparency of foreign legal arrangements.

b) Armenia has carried out the risk assessment of domestic and foreign legal persons (all), and of legal arrangements. The indicators used are all relevant, with additional scope for analysis needed in assessing the rationale of having domestic and foreign legal persons with no relationship with a reporting entity.

c) The State Register Agency maintains the State Registry which holds basic information on the Armenian legal persons and where available, BO information. Law enforcement and supervisory authorities have direct access to the State Registry which allows for accessing adequate, accurate, and up-to-date basic information, and when available, BO information.

d) A multi-pronged approach to access BO data is used through three main sources: (i) information held by the reporting entities, mostly banks; (ii) information contained in the State Registry, and (iii) information held by the legal persons. Effectiveness of the multi-pronged approach would benefit from further development given that the State Registry is not yet fully populated, and the absence of a legal requirement for legal persons to have a bank account.

e) LEAs do not have direct access to financial information from reporting entities but can access it through a court order or through the FMC. As from June 2021, BO information can be also obtained from the legal persons themselves, who are obliged to provide the information within five days, but this option is rarely used in practice.

f) Armenia does not recognise trusts and similar legal arrangements; thus, trusts cannot be created under Armenian law. However, trustees of a foreign law trust or persons holding an equivalent position, can operate in the country. Armenia assesses exposure to foreign legal arrangements as low, which is as expected in view of the very limited materiality.

g) During 2021 to 2024 1,903 administrative proceedings were initiated against legal persons, of which nine were for incorrect or incomplete information, and the rest for failure to submit BO information to the State Registry. Of these, 39% led to remediation

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

measures, which is a positive outcome. In the rest of the cases, the imposed sanctions (mainly warnings) do not appear to be neither dissuasive nor effective. Armenia has also imposed forced liquidation in a one-off initiative in 2016, to approximately 30,000 dormant legal entities.

Key Recommended Actions (KRA)

a) Authorities should enhance their understanding on domestic and foreign legal persons' vulnerabilities of (i) not having a fully populated BO registry, (ii) absence of checks on the accuracy of the BO information, (iii) rationale of having legal persons with no relationship with a reporting entity, and (iv) TF geographic vulnerabilities considering the residency of the BOs/founders and the country of registration of BO/founder.

b) The State Register Agency should carry out systemic verification checks of the accuracy and relevance of BO information on a risk-based approach, to ensure its reliability and mitigate the risks of the creation of legal persons for ML/TF purposes.

Other Recommended Actions

Authorities should:

a) ensure that there is a combination of mechanisms that enable the timely access to adequate, accurate and up-to-date BO information of foreign legal persons having sufficient links to Armenia and posing ML/TF risk.

b) proceed with the monitoring and forced liquidation for the inactive legal persons registered in Armenia following the one-off similar exercise performed in 2016.

c) adopt measures to ensure that there is greater transparency in the use of nominee arrangements to prevent abuse of these mechanisms for ML/TF.

d) ensure that there is a discrepancy reporting mechanism for BO information and provide more guidance to the reporting entities on what this effectively implies.

e) assess and address the vulnerabilities in relation to the criminal liability of legal persons.

Overall conclusion on IO.5

The ML/TF risks related to legal persons were assessed in the 2024 NRA, with the conclusion that the legal persons most frequently used in criminal activities are the LLCs, closed joint stock companies (JSCs), and, in some cases, non-profit organisations (NPOs). All domestic legal persons must be registered with the State Registry. Basic information is publicly available and includes personal identification details, such as addresses, citizenship status, and birth/death records, along with company ownership, registration details, and tax status for businesses. The most significant development to prevent the misuse of legal persons and to increase transparency of basic and BO information, was the setup of the electronic BO Registry that is being gradually populated with BO data since 2021 (50% completed at the time of the on-site visit). There are no systematic verifications and checks on the accuracy of the BO data. The BO data is also held by FIs and the information kept therein is generally of a good quality, notwithstanding that deficiencies have been identified by the supervisors. Concerning foreign legal persons, a key vulnerability identified was the identification of the BO. The materiality of foreign legal arrangements does not appear to be significant. Administrative sanctions imposed do not appear as being dissuasive and effective, especially in view of the fact that the register is still half populated with the BO data.

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

302. A wide range of legal persons can be formed in Armenia including LLCs, Closed JSCs and Open JSCs, cooperatives, and partnerships (which can be either general or limited partnerships and with no general partnership established since 2014). LLCs are the most material[66], accounting for 85% of the total registered companies, followed by public organisations (5.7%), and closed JSCs (2.5%).

303. Since the previous MER, Armenia's system for capturing basic and BO information for legal persons has undergone a series of reforms, mainly legislative. In June 2021, a law was adopted introducing rules for recording information on BO of legal persons in the State Registry. The obligations to declare BO were implemented gradually through transitional provisions, and from 1 January 2023, they apply to all legal persons registered in Armenia, including those registered before adopting the law.[67]

304. Ownership and identity information in relation to legal persons is available from the State Registry, while ownership and identity information in relation to JSCs is available from the Central Depository.

305. Trusts are not recognized in Armenia, so domestic legal arrangements cannot be created under Armenian Law. Although nothing precludes foreign legal arrangements (e.g., trustees of a foreign law trusts) to operate in Armenia, very few (if any) such cases have been reported.

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

ML risks – Legal persons registered in Armenia

306. The ML/TF vulnerabilities of the legal persons were assessed in the 2024 NRA through a working group composed of the Ministry of Justice, the State Register Agency, the FMC, the prosecutors' office, the NSS, the Investigative Committee, the State Revenue Committee (tax authority) and the anti-corruption committee. Various sources of information were used, such as i) statistics on registered legal persons and their features, ii) data received from reporting entities, iii) information from LEAs, iv) STRs received by the FMC, v) survey responses and notifications provided, and vi) strategic measures aimed at reducing the ML/TF vulnerabilities of legal persons.

307. The legal persons most frequently used in criminal activities are the LLCs, closed JSCs, and, in some cases, non-profit organisations (NPOs).[68] LLCs are the most exposed to ML, especially when a non-resident BO is involved. LLCs are also preferred due to their legal features, as criminals seek to avoid personal financial risks by exploiting the company's limited liability. The closed JSCs' ML/TF vulnerabilities are not explained in the NRA, and authorities did not present typologies in this sense.

308. During 2021 to 2023 a year-over-year increase in the number of legal persons involved in investigations was noted.[69] The involvement of legal persons in ML schemes was mainly linked to tax and corruption-related crime, including various forms of embezzlement, where legal persons were used

[66] As of October 2025

[67] 2024 NRA, par. 248

[68] 2024 NRA, par. 754

[69] 2024 NRA, par. 757.

to conceal the traceability of their criminal activities. LEAs have difficulties in holding the legal persons criminally liable as no investigations have been initiated against legal persons for ML or related offences, and no conviction of legal persons has been achieved as yet since the introduction of corporate criminal liability (in force since 2023). This vulnerability is still to be explored (see IO7).

309. The risk assessment features a number of typologies where "shell" companies LLCs, were used to open bank accounts, and where funds of unknown origin were transferred through these accounts to legal persons registered in offshore jurisdictions.[70]

310. Authorities report that although legal persons appear in STRs, FMC notifications, formal and informal requests for information, criminal cases, court proceedings, and convictions, the overall ML vulnerability remains at the level of moderate.

311. Turning to the foreign ownership of Armenian legal persons, the primary countries of origin of the owners/shareholders, and BOs of Armenian-registered entities include Russia, Iran, India, the UAE, the USA, and Georgia.[71]

312. The authorities cross-checked data from the State Registry and data from the reporting entities (mainly banks) and found that from the 15,234 LLCs registered in Armenia with a foreign BO or shareholder, only 7,135 (47%) performed at least one bank transaction during 2021-2023. Authorities concluded that this indicates that over 50% of the legal persons registered in Armenia with a foreign founder, manager or BO do not in practice conduct economic activity in the country and did not engage in transactions with reporting entities.

313. The 2024 NRA found that resident and non-resident legal persons are primarily used for both cross-border and domestic money transfers, with resident legal persons also engaging in cash transactions.[72] This finding shows that the effectiveness of the law on non-cash transactions in effect since July 2022 is questionable. The authorities should further explore the risks related to the use of cash by legal persons and the impact of the law on non-cash transactions.

314. Data presented by the authorities indicated that 63% of the total legal persons registered in Armenia are not active. Dormant legal persons retain legal personality and have no limitation in their registration. Most authorities reported that there are no ML/TF risks attached to these companies as they do not conduct any business activity[73]. Authorities also clarified that the reason for the existence of such high number of dormant (also called "inactive") companies is that the liquidation procedures are legally complex, being easier and cheaper to leave a legal entity dormant than to apply for liquidation. Companies are given the status of dormant or inactive in the SRC's (tax authority) database, and the State Register Agency has no visibility over the "dormant" status of the company unless it applies for liquidation or termination.

315. Following the on-site, Armenian authorities reported that they looked at the STRs received, requests from LEAs, informal and formal international requests, and criminal investigations and found no case involving dormant legal persons. Moreover, the FMC reported that they cross-checked the threshold transaction reports (TTRs) against the SRC database and learned that between January–September 2025, only 56 dormant legal persons conducted a total of 142 transactions via banks with the aim of repayment of loans. The AT commends the authorities for the efforts put into understanding

[70] Armenia has a list of countries with special liberal taxation systems.

[71] 2024 NRA, par. 738.

[72] 2024 NRA, par. 756.

[73] In later stages of the assessment, the authorities have presented statistics for 2025, showing that the SRC has flagged and subjected 391 inactive legal persons to supervisory actions. 167 taxpayers have been found to be in breach of tax obligations. No ML/TF risks have been identified.

the nature and the rationale behind the high number of dormant companies and recommends the State Register Agency to continue with the forced liquidation in order to address this vulnerability.

316. Nominees are not recognised by the Armenian legislation but in practice there are cases of "straw men" acting as managers/owners of legal persons. A form of "nominee" arrangement is possible in case of JSCs, in the form of custodians who are in the majority of the cases, reporting entities. Those are however licenced/certified but not monitored and not assessed in the NRA. Authorities are not aware of cases where such arrangements are used in practice.

ML risks – foreign legal persons with sufficient links to Armenia

317. The authorities looked at the risk related to the foreign legal persons with sufficient links with Armenia by requesting information from reporting entities, SRC (tax authority), CBA, and Cadaster Committee (real estate state registration). A wide range of criteria were considered to determine the sufficient links to Armenia: type of business activities, the existence of a business relationship with reporting entities, the existence of a local physical establishment (branches and agencies), real estate investments, country of origin of BOs, and the existence of BOs (or similar functions) of Armenian nationality.

318. Foreign companies that attain permanent establishment status in Armenia are required to register for tax purposes with SRC by providing their Articles of Association. Ownership information will be available therein to the extent that the laws of the jurisdiction of incorporation so require.

319. The Cadastre committee, which is responsible for the real estate registration, collects basic information, including the country of registration when a foreign legal person acquires real estate properties in Armenia. BO information is not collected.

320. The authorities' analysis concluded that the number of foreign legal persons with sufficient links with Armenia stood at 1,586, of which 34 (2%) maintained a branch or representative office, 1,060 (66%) conducted economic activity in Armenia; 89 (5%) maintained ongoing business relationships with reporting entities; 91 (6%) owned real estate in Armenia; 258 (16%) owned investments in Armenia; and 102 (6%) had an Armenian BO or shareholder. Out of the 1,586 foreign legal persons, the most common type of companies were LLCs.

321. Main countries of registration of the foreign legal persons with a sufficient link to Armenia were Russia, Cyprus, Iran, UK, France, US and the UAE. Foreign legal persons registered in offshore jurisdictions accounted for 5% of the total foreign legal persons.

322. Authorities reported that that during 2021 to 2023, there were 12 criminal proceedings involving foreign legal persons including those with no sufficient link to Armenia. A key vulnerability identified by LEAs, which is also evident in the case studies presented to the AT, concerns the difficulties in identifying the BOs of foreign legal persons for both entities with and without sufficient links to Armenia.

323. Given the limited number of cases involving foreign legal persons, authorities reported a low ML/TF risk. Although the AT considers this analysis relevant and reasonable, there are some gaps that might impact its completeness in that: i) subsequent changes in ownership of the foreign legal persons that attain permanent establishment status in Armenia would not be available to the SRC (tax authority); ii) there is no register of BO data of foreign legal persons and (iii) no multi-pronged approach given that not all the legal persons have a bank account.

All legal persons – ML risk assessment

324. The AT sees the sources of information used in the ML risk assessment as reasonable. However, there remain aspects that are not fully analysed, and that impact the vulnerabilities of legal persons: the

impact of not having a fully populated BO registry, the accuracy of BO information given the absence of checks (at a minimum random or risk based), the number and rationale of having legal persons with no relationship with a reporting entity, as well as the minor deficiencies in the risk assessment of the foreign legal persons with links with Armenia.

TF risk assessment

325. Authorities found the TF-related vulnerabilities of legal persons as low on the basis of the absence of cases of TF involving legal persons; low number of legal persons, their associates or BOs from jurisdictions assessed as high-risk from a TF perspective, and absence of international formal and informal requests related to TF, and criminal proceedings and convictions with TF offences. Nevertheless, the AT has concerns regarding this overall conclusion mainly because according to the geographical distribution, 6% of the domestic legal persons have owners or BOs, or are companies incorporated in a country blacklisted by the FATF.

ML/TF risks – Legal arrangements

326. Legal arrangements cannot be created in Armenia. Reporting entities confirmed that there are no trusts or other form of legal arrangements among their clients. Therefore, together with the absence of trusts in formal and informal international requests, and in criminal cases, this led to a low ML/TF risk of legal arrangements.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

327. The most significant development to prevent the misuse of legal persons to increase transparency of basic and BO information during the reporting period, was the setup of the electronic BO Registry that is being gradually populated with BO data since 2021. Additionally, the State Register Agency has started supervising compliance of the obligation to identify and provide the BO information, and as from 2023, the State Register Agency started initiating administrative proceedings for submitting incorrect or incomplete information in the BO declaration form.

328. At the time of the onsite there was no data or analysis related to tax audits conducted on dormant legal persons that were reactivated[74]. Authorities report that as a mitigating measure any domestic transactions of dormant companies would change the company status at the tax authority and trigger attention.

Domestic legal persons
Basic information

329. All domestic legal persons must be registered with the State Registry. Basic information must be provided by the chief of the executive body of the legal person or whoever this person so authorises. The applicant can complete the information independently or with the assistance of a representative of the state authority at an office of the State Register. There is no requirement on legal persons to hold basic information.

330. Basic information includes personal identification details, such as addresses, citizenship status, and birth/death records, along with company ownership, registration details, and tax status for businesses. The personal information of owners and executive directors is checked for accuracy upon registration by the State Register Agency using national databases in case of Armenian nationals and

[74] *In later stages of the assessment, the authorities have presented statistics for 2025, showing that the SRC has flagged and subjected 391 inactive legal persons to supervisory actions. 167 taxpayers have been found to be in breach of tax obligations. No ML/TF risks have been identified.*

translations of identification documents in case of foreigners. The basic company information is publicly available and free of charge.

331. For JSCs, legal ownership information is inputted in the system by the Central Depository account operators, which are financial institutions, and includes at least the following information about each individual shareholder/legal owner: full name, father's name, ID information, residence address, account reference, account type (whether securities or cash accounts), contacts, nationality, date of birth, bank account. In case the shareholder/ legal owner is a legal person: full trade name, state registration data, principal place of business (mailing address), personal name of the head or representative of the legal person and contact details.

332. The Central Depository as a reporting entity supervised by the CBA, verifies the information in line with its AML obligations.

BO information

333. By 2023, BO information of all legal persons is submitted electronically through the online platform of the State Registry. At the stage of logging in, the platform verifies the identity of the person submitting information on behalf of the legal person. Information already contained in the State Registry (basic information) is auto filled by the system to avoid human negligence. The person is then prompted to fill-in required sections of the declaration. A section, as well as specific cells of the form may activate or deactivate based on data inputted by the user. Additionally, some cells are formatted and allow only limited types of input, and drop-down boxes are used, where possible, to avoid manual input of information. The legal person is obliged to declare the BO/s to the State Registry within 40 days of its registration, report any changes within 40 days and then confirm or make changes to the BO/s previously declared at least once a year. The BO data is automatically registered only if all the fields of the electronic form are completed.

334. Following the submission, the BO data is automatically recorded in the State Registry database. The BO declaration is automatically checked for apparent mistakes and is published within two working days.

335. The details to be provided include: (i) information on BOs: full name, citizenship, date of birth, address and contact details, (ii) details of the identity document (which are attached in case of foreign nationals), (iii) grounds for being a BO and details (percentage of shares, direct or indirect participation, other means of control, individual or joint control, or manager) and (iv) when there is a chain of ownership, information on all the intermediate legal persons (name, registration number, address, jurisdiction of registration, and name of head of the executive body).

336. The State Register Agency does not verify the accuracy of the information contained in the documents except to check that the documentation provided matches data included in the application form.

337. From the data that was presented, 49 per cent of the legal persons still did not provide BO information and the authorities explained that the non-declarations are predominantly related to the dormant legal persons. Following the on-site, authorities explained that they looked at the BO population through the prism of the active/inactive companies by cross-checking with the SRC (tax authority) and concluded that 82% of the active companies have declared their BO.

338. Reporting entities are obliged to identify the BO in their CDD process, and update data collected at a self-determined periodicity on a risk basis, which should be at least once a year, to ensure that it is up to date and relevant. The information stored therein is generally relevant and kept up to date, with the deficiencies identified in IO.3 and IO.4. While this constitutes a meaningful mitigating measure, it is be noted that there is no requirement for legal persons to have a bank account in Armenia, or to involve a reporting entity at incorporation stage or throughout the life of the business. This shortcoming

is mitigated by the adoption of the Law on Non-Cash Transactions adopted in 2022, whereby all the transactions between legal persons concluded and/or paid in Armenia must be executed by non-cash means. This implies in practice that active legal persons should have a bank account, however this data was not provided during on-site. Certain exemptions exist, for example, payments below circa Eur700, and transactions for acquisition of goods formulated in a VAT return account, written off by foreign citizens and stateless persons.

339. During the on-site, supervisory authorities reported that there are several legal persons that declared as BO the official carrying out the overall or current management of the legal entity's activities, and they found nothing unreasonable about this. Authorities reported that it is expected and reasonable that state-owned enterprises and non-commercial legal persons to declare this type of BO. Post on-site, authorities clarified that as at October 2025 there were 42,442 BOs that may fall under this definition (the official carrying out the overall or current management of the legal entity's activities). It was then further provided that out of this figure, 7,067 declared exclusively as BO the official carrying out the overall or current management of the legal entity's activities.

340. While the Anti-Corruption Strategy for 2023-2026 and the National AML/CFT Strategy for 2025-2028 foresee the development of a discrepancy reporting mechanism, this has not been effectively implemented.

341. While noting that no guidance has been issued by the State Register Agency on how BOs should be identified, the Agency considers that the Central Bank Guidance[75] published in 2024, is of assistance to legal persons and reporting entities in determining the BO. This guidance explains that when reporting entities cross-check with the State Registry and detect inconsistencies in the BO data, they should "*provide an opportunity to make relevant alterations to the State Register within a reasonable but unspecified time limit, and in case of uncooperative behaviour of the legal person, it should, based on part 1 or 2 of Article 27 of the AML/CTF Law, reject the transaction and not approve (terminate) the business relationship*". The text of the Guidance is informative for the SRA in that they will be notified by the RE in case of an inconsistency detected but does not provide assistance in how to identify the BO by themselves. Also, the AT notes that there is no reference in the guidance document whether a suspicious report should be filed in cases where the transaction is rejected. During the on-site some of the reporting entities confirmed that they report the found discrepancies to the State Register Agency, but no statistics are kept in this regard to estimate the accuracy of BO information. Although no records are kept on the number of such instances, the authorities maintained that the discrepancies were negligent mistakes and not attempts to conceal the BO.

342. Legal persons are not subject to any type of oversight mechanism (i.e., on-site checks) to ensure that a company is not a shell company.

343. In public procurement, the legal persons bidding on state contracts must submit a BO declaration.

Foreign legal persons with sufficient links with Armenia

344. With regards to foreign legal persons with sufficient links to Armenia, basic and BO information can be sourced from reporting entities to the extent that they engage in business relationships or an occasional transaction with an FI or DNFBP.

All legal persons and legal arrangements

345. Overall, Armenia took some key relevant mitigating measures to prevent the misuse of legal persons for ML/TF purposes, such as the electronic register (State Registry) for both basic and BO information, the Central Depository and the obligation to identify the BO placed on the reporting

[75] 20241022_BO Guide_ENG.pdf

entities. However, no systematic verifications were carried out by the State Register Agency on the accuracy of the BO information. When discrepancies were reported to the State Register Agency by the competent authorities, the Agency imposed nine administrative sanctions (6 in 2023 and 3 in 2024) for incomplete or incorrect information. There is no data on the same that were reported by the reporting entities as explained above.

346. Although reporting entities are requested to hold BO information on legal arrangements since only recently (prior to the legal amendments the definition in the law of what constitutes a trust was not in line with what is requested in c.25.4), these entities are of low materiality in Armenia.

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

Domestic legal persons

Basic information

347. Basic information in the State Registry is publicly available online. All documents submitted to the State Registry since 2012 are accessible electronically and those submitted before are in the process of being digitalised. The State Registry contains comprehensive basic information on the founders of all companies, partnerships and co-operatives.

348. Changes to basic information take effect only after registration in the State Registry. After registration, up-to-date legal ownership information is available with the State Registry for LLCs, co-operatives and partnerships, and with the Central Depository or custodians for JSCs. A legal person is considered as established from the moment of state registration.

349. There is no direct requirement for updating of legal ownership information of legal persons in the State Registry, however the State Registry contains past and current basic information of (active) LLCs because any changes to capital compositions or shareholding acquire legal force vis-à-vis third persons from the moment of their state registration.

350. Information about founders and participators of JSCs is also recorded in the State Registry; however, all subsequent changes are not registered therein as there is no obligation to amend the articles of association when the membership changes. The changes in ownership of shares in JSCs (both open and closed) are registered with the Central Depository.

351. Information contained in the Central Depository is adequate, accurate and current and is available to the representatives of the JSCs, their shareholders, CBA (including FMC) and LEAs. Representatives of the JSCs and their shareholders can access the information by submitting a request to the CDA via the CDA account operators and the information is provided by the CDA within five days.

BO information

352. Armenia uses a multi-pronged approach to access BO information through three main sources: (i) the data contained in the State Registry; (ii) the data held by the reporting entities; and (iii) as of June 2021 data held by the legal persons themselves.

Information contained in the State Registry

353. Since 2021, the State Registry started to be populated with BO information which includes sufficient data for their identification.

354. Supervisory authorities and LEAs have direct access to the BO information in the State Register. However, in practice they appeal to the reporting entities to access BO information as the Registry is not fully populated.

Information held by the reporting entities

355. LEAs (except SRC (Tax Unit)) have access to BO information kept by the reporting entities

(mainly banks) on the basis of a court order. LEAs reported that this generally is not a lengthy process and addressed within a few days.

356. LEAs can also access BO data held by reporting entities (mainly banks if the legal person has a bank account) through the FMC, where the information was reported to be shared in three to four days.

357. No records are kept of the number of BO information requests made to the reporting entities or to the FMC, nor on the completeness and swiftness of the replies.

358. Basic and BO information of foreign legal persons that have sufficient links to Armenia can be accessed only through the reporting entities who are obliged to identify them in the course of the CDD process. FMC and SRC have direct access to this information. The other competent authorities (mainly LEAs) have to appeal to a court order.

Information held by legal persons

359. With the legal amendments in June 2021, legal persons are also subject to record-keeping obligations in relation to BO information and are required to make this information available within five days to the competent authorities. There is little use of this option in practice.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information

360. Since August 2025, with the legal amendments, that amongst others, clarified the definition of trusts, reporting entities have the legal obligation to keep basic and BO information of foreign legal arrangements that have business relationships with them. No such business relationships have been reported by the Armenian authorities, which is consistent with the conclusion of minimal low materiality in the country.

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

361. With the amendments in the State Registration law in June 2021, the registrant is liable for providing false information as well as for the subsequent consequences, with sanctions consisting in warnings and fines (refer to criterion 24.14). For submission of false information and concealment of information about BOs, the authorized person may be liable to warnings, fines, short-term detention or prohibition to perform certain activities for up to three years. Legal persons can also be forcibly liquidated by the court if they fail to provide their declarations for three years in a row. Criminal penalties may be applied (refer to criterion 24.14) on participants of the legal person or the BO for providing false information to the legal person, or concealing information subject to submission, or for the failure to respond to the inquiry of the legal person.

362. As a consequence of the supervisory actions undertaken by the State Register Agency as shown in the table below, during 2021 to 2024 1,903 administrative proceedings were initiated against legal persons, of which nine were for incorrect or incomplete information, and the rest for failure to submit BO information to the State Registry.

363. As a result of the Authorities' initiative on the application of warnings, 39% led to remediation measures, which is a positive outcome. In the rest of the cases, it was not monitored whether the imposed sanctions (mainly warnings) were followed by remediation measures or not. The authorities reported that the fine imposed was that of around Eur70, which does not appear to be neither dissuasive nor effective. In fact, the 2024 NRA identified as a vulnerability the low penalty for failure by the legal persons to retain the accounting documents, which enables criminals to erase traces of their crimes, thus creating challenges for LEAs in gathering evidence in criminal cases. The amount of the penalty imposed is the same as that for legal persons not retaining BO information.

364. Armenia has also imposed forced liquidation in a one-off initiative in 2016, to approximately

30,000 dormant legal entities.

Table 5.1: Administrative proceedings (2021-2024)

	2021	2022	2023	2024
Initiated administrative proceedings	150	1118	435	200
Imposed sanctions	15	115	27	103
Terminations based on achieved compliance	130	300	221	91

365. The authorities recognise that more resources and capacities are required to conduct increased and effective administrative monitoring especially in view of the registered legal persons that still need to declare their BO.

366. In view of the above data and the amount of BO declarations that still need to be submitted, (even if considering only the active companies), Armenia should enhance its efforts in supervision and enforcement action taken to ensure the availability of BO information in all cases and continue with of forced liquidation of dormant.

Chapter 6. Financial Intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The Armenian FIU has increased its capacity in recent years, both in human and IT resources. The FIU receives STRs, threshold-based disclosures, information on identified non-disclosures of cash at the border, and cash declarations, which are used in the course of operational and to some extent strategic analysis. The FIU remains a key source of information otherwise subject to bank confidentiality provisions by other authorities, especially at the level of operational intelligence activities.

b) STRs form the primary source of FIU analysis. The FIU has taken steps to enhance the quality and structure of STRs through various feedback mechanisms. Nevertheless, although the most material sector (the banks) is the primary reporting sector), the overall reporting level of STRs is insufficient, in particular among DNFBPs. The STRs received from FIs generally possess the relevant information and are aligned with the main ML/TF risks signalled in the NRA, with some exceptions (e.g., drug trafficking).

c) The FIU plays an important role in supporting LEAs by providing information for their operational intelligence and investigative activities. LEAs generally consider the FIU financial intelligence to be of good quality. Strategic analysis supports the needs of other competent authorities too. The FIU does not use analytical IT tools to conduct thorough financial analysis and network analysis based on data from different sources. Additional staff is needed to further enhance strategic analysis. Overarching responsibilities of some of the LEAs conducting operational-intelligence activities makes the decision on selection of the recipient of a spontaneous dissemination of financial intelligence prone to subjectivity.

d) While LEAs, in particular the intelligence-gathering agencies, regularly request information from the FIU, the significant share of these requests focus on cases concerning predicate offences rather than ML. Such support often involves conducting financial analysis and information from foreign counterparts and reporting entities, which strained FIU resources in previous years. The intelligence bodies – main recipients of FIU information - enrich FMC data in the course of operational intelligence activities. Results of their analysis indicate they primarily pursue the predicate offence and do not include the ML hypotheses.

e) Authorities cooperate and exchange information and financial intelligence via secure channels and mechanisms. The FIU actively engages with other competent authorities both through the Interagency Committee, ad hoc joint teams, and bilateral meetings. Memoranda of Understanding have been signed with key FIU stakeholders to facilitate cooperation. The FIU IT environment and established safeguards protect the confidentiality of the information processed.

f) The current trend of the increased use of STRs tied with the rising number of FIU notifications (spontaneous disseminations) to LEAs is positive. The number of ML investigations originating from disseminated FIU intelligence has risen, especially in the years 2023-2024. In total, the FIU provided assistance in 73% of all ML investigations There are concerns about the effective use of financial intelligence by LEAs at the intelligence gathering phase, before the case is referred to investigative authorities to initiate a criminal proceeding.

Key Recommended Actions (KRA)

a) The intelligence bodies (NSS, MIA, SRC, ACC in the intelligence capacity), as primary recipients of FMC disseminations, and as responsible authorities for initiating ML cases, should focus more on the ML aspect in their intelligence gathering activities. Specialised officers should be trained on systematically developing and using financial intelligence and tracing criminal proceeds related to ML/FT.

Other Recommended Actions

a) The FMC should further enhance its operational analysis by:

- establishing internal guidelines to assist in determining the best suited recipients of FMC notifications;
- acquiring IT tools necessary to conduct thorough financial analysis and network analysis based on data from different sources;

b) The FMC should further enhance its strategic analysis capabilities by increasing resources of the relevant division and boosting its capacity, through training and relevant IT tools for data analysis.

c) The FMC should continue to monitor the level or reporting of STRs from DNFBPs and engage in outreach activities to notaries, casinos gambling operators and real estate agents, to raise awareness on their responsibilities and abilities to reporting ML/TF suspicions.

d) The authorities should review LEAs access to financial information for ML in intelligence purposes (e.g. considering granting access to the central bank account register).

Overall conclusion on IO.6

The FMC possesses broad access to critical datasets, including the Central Bank Account Register, tax databases, criminal records and real estate records. While STRs are the primary driver of analysis, the FIU also utilizes TTRs, domestic/foreign requests, and open-source intelligence. The volume of STR reporting requires improvement in order for the FIU to better support the operational needs of competent authorities.

Other authorities in their intelligence gathering activities have timely, accurate and up-to date access to relevant information. The absence of LEA access to the bank accounts registrar unnecessarily prolongs the access to financial intelligence and puts a burden on the FMC. Although the FIU provides high-quality intelligence to LEAs, its resources have been strained by a high volume of requests focused on predicate offenses rather than money laundering (ML). Additionally, analytical results of intelligence bodies rarely support the

ML hypotheses due to gaps in specialized training and time constraints. While strategic analysis is generally effective, it remains limited by current resource and software capabilities. There is a positive upward trend in the utilization of STRs and FIU notifications within ML investigations.

Armenia is rated as having a moderate of level of effectiveness for IO.6.

367. Since the last MER in 2015, Armenian authorities have taken numerous steps to strengthen the production of financial intelligence, foster interagency cooperation and expand the set of data the FIU and the relevant intelligence bodies have access to. The assessment of the effectiveness of the measures in place was based on provided statistical data, system demonstrations, discussed case studies and results of interviews with Armenian authorities and representatives of reporting entities. Relevant findings from related immediate outcomes were also taken in account to support the conclusion.

6.1. Timely access to relevant, accurate and up-to-date information

6.1.1. By the FIU

368. The FMC has access to a broad range of information for conducting operational and strategic analysis both via reports received in the form of STRs, TTRs, cash declarations and access to the relevant financial, administrative and law enforcement databases.

Reports received

369. Since the previous MER the number of STRs slightly increased, from 254 in 2020 up to 366 in 2024 (44%). The significant majority of these (on average 77%) come from the banking sector, which is the most material. A further 8% originates from entities engaged in money (currency) transfer services. The rest of FIs have provided a handful of reports. With regard to DNFBPs, casinos have prepared in total 57 reports (3% of all disclosures), while notaries 184 (11% of all disclosures), with other sectors filing STRs rarely. The overall level of reporting by the private sector is an area for improvement. There are no STRs filed by real estate agents and VASPs.

370. Reports from FIs, which form the majority of received STRs, are partially in line with the risk and materiality but generally include the necessary content and suspicion reasoning. In order to improve the quality of submitted reports from the banking sector, the FIU has systematically provided both general and individual feedback, which was also shared with to the AML/CFT supervisory wing of the CBA (FSLD). The monitoring conducted by the FIU since 2021 show a gradual improvement of STRs, content-wise and form-wise. When STRs would benefit from additional information, the FMC staff can request the relevant information from REs to support analysis.

371. Looking at the source of reports disaggregated by sector, the reporting of non-bank FIs and DNFBPs (excluding notaries) has been declining. The authorities associate this with various factors, including limitation on use of cash in the economy and functional restrictions[76] . Another reason for the decreasing STR reporting is linked to the guidance provided by the FMC discouraging reporting from financial institutions, in the cases of potential proceeds of crime originating from small-scale fraud. This was done as in the perception of the FIU those STRs added limited value for the FIU intelligence. Such reports would go directly to the Police on the basis of a victim complaint. Turning to quality, the majority of DNFBP reports do not contain the relevant level of suspicion or information necessary for the FMC to develop intelligence products There is a need for continuous monitoring of suspicious transaction reporting behaviour and further engagement to guide the REs, in particular DNFBPs into

[76] for example, an e-wallet cannot be funded with more than 1 million Armenian dram – around EUR 2,200 EUR – and e-wallets or gaming accounts can be funded only through cashless methods

increasing their reporting level and the quality of the STRs.

Table 6.1. STR reporting trends

Entities	2020	2021	2022	2023	2024
Banks	196	224	209	268	273
Entities Engaged in Money (Currency) Transfer Services	32	27	25	24	12
Entities Providing Investment Services (Investment Companies)	1	2	0	1	7
The Central Depositary	3	1	0	1	2
Credit Organizations	3	2	3	0	0
Entities Engaged in Foreign Currency Exchange	0	0	0	1	0
Insurance (Including Reinsurance) Companies77	0	0	0	0	1
Casinos (Including, Organizers of Games of Chance and Lotteries)	18	6	17	4	12
Sole Practitioner Lawyers and Legal Firms	0	0	0	1	0
Notaries[78]	1	0	0	125	59
Total	254	262	254	425	366

372. The nature of the STRs varies considerably, particularly between sectors. Reports received from FIs are generally commensurate with the main ML risks highlighted in the NRA, although the number of reports involving potential drug trafficking identified by the FMC are limited. The authorities explained that this may be due to the fact that reporting entities are tying STRs with other crimes or have no indication on that the underlying predicate. The absence of regulation of VASPs is another reason.

Table 6.2. STR from FIs by predicate offence

STRs from Fis	Total (ML/TF/ML & predicate offences)	TF	Fraud	Drug trafficking	Corruption	Tax evasion	Other crimes	No crime specified
2021	256	2	27	2	6	27	11	181
2022	237	1	29	1	6	12	5	183
2023	295	2	32	1	10	33	5	212
2024	295	0	69	3	16	44	13	150

373. The FMC provides complete feedback to RE annually, in form of i) general feedback, with an overall summary and evaluation of the reports submitted by the respective RE, supplemented by ii) individual feedback on each STR from the following perspectives: form, content, other contextual factors, priority, actions taken by the FMC, and descriptor of dissemination. In addition, the FMC assesses the submitted STRs in terms of their alignment with the characteristic indicators and risk profile of the respective RE. The RE is obliged to provide an explanation for the deficiencies identified in the feedback process, as well as the steps taken to improve the STRs. If necessary, face-to-face meetings and discussions are also organized with particular REs. Apart from annual feedback, the FMC may also provide ad-hoc targeted feedback on particular reports or specific groups of STRs (for example, STRs concerning cash transactions from a particular RE, which lacked detailed analysis).Since 2020, five TF-related STRs have been received, all relating to potential matches with lists of entities involved in possible terrorist or similar activities abroad. Ultimately, no connections with designated persons were

[77] Non-life insurers outside the scope of the Methodology
[78] Notaries have filed a considerable number of reports, but when analysing their value, the authorities concluded that this category of STR were bearing little value for two reasons: on one hand the STRs were emanating mostly from two notarial offices located in a specific area of the country and, on the second hand the suspicions contained therein were not relevant (donations between family members or vague reason for suspicion).

confirmed in the course of FIU analysis.

374. In addition to receiving STRs, the FIU engages in a periodic TF strategic analysis codenamed “Regional level operation”, which envisages the collection of data on outgoing and incoming money transfers made from Armenia to a number of jurisdictions identified as being at relatively higher risk of TF through fast money value transfer systems via banks. The collection of this data (which usually deals with low volume and low intensity transfers) is then followed by a FIU analysis for the purposes of identifying any possible trends, tendencies or developments associated with jurisdictions identified as having heightened TF risks. Information on suspicious transfers to risk areas have been disseminated to the NSS. None of these transfers were previously reported as STRs (see IO.9).

375. The AML/CFT provisions govern strict rules on the timeframe for reporting suspicious transactions and activities. While the FMC has not identified many cases of delays in the transmission of STRs by the banking sector, limitations in the sphere of supervisory activity regarding non-banking financial sector and DNFBPs, negatively impact the quality and the quantity of the STRs emanating from this sector. Supervisory actions conducted on FIs identified cases of non-reported STRs gives the indication that the overall number of STRs is an area for improvement (see IO.3 and IO.4).

376. Apart from STRs, the FMC also receives other disclosures, such as threshold- reports based on objective criteria (TTRs – see table below) and declarations of cash and BNIs across the external border. During the period under review, a total of 3,770,154 TTRs were received by the FMC with banks accounting for 92% of them. The increase in TTRs submitted by notaries is due to legislative changes in November 2023, requiring submitting TTRs for donation transactions. As for cross border declarations, the FMC received around 4,700 reports (incoming and outgoing) along with around 100 reports concerning non-disclosures. Those reports contain relevant, accurate and up to date information, which is used in the operational and strategic analysis.

Access to databases

377. Besides the reports described above, the FMC has access to a broad range of different information sources in order to perform its functions. Information directly accessible to the FIU:

- ACMS, including data from FMC analytical cases (STRs, requests from counterparts, etc.), list of identified local and foreign VASPs, list of persons related to TF/PF, etc.
- Centralized bank account register
- Credit registry
- Court decisions on LEA access to confidential banking information
- Passport database
- Database of State Revenue Committee (salary, workplace, position etc.)
- Database of Social Security Service
- BO register
- State register of legal entities
- Real estate database
- Database of Civil Acts Registration Service
- Administrative proceedings of Road Police
- Compulsory Enforcement Service (confiscations)
- Vehicle/ driving license database
- Police database (criminal records)
- Registry of licensed weapons
- Database of disability benefits

378. The FMC has developed its Automated Case Management System (CMS) to allow one-click access to information administered by the FIU (STRs, TTRs, subjects in cases) and twelve other external

sources, for example the State Register, real estate database, vehicle register or SRC database. This data is automatically collected in the course of a single inquiry made in the CMS. Other information sources, such as the centralized bank account register, have to be accessed using a separate interface. Open sources and commercial databases are checked on a regular basis. Other sources, such as border-crossing data, are verified in accordance with the nature of the case.

379. Information on request can also be obtained from reporting entities, even if they have not submitted a STR. According to the FIU operational manual, when sending additional information requests, a deadline for responding is set, which in practice is respected by the recipients. For example, in the case of banks, the deadline is one business day for urgent requests and three business days for non-urgent requests. The FIU can also request information from other intelligence bodies and supervisory authorities. This power is used only in particular cases due to the FIU's wide access to law enforcement and supervisory information and can take several days (for example in case of the need to obtain tax declarations from the SRC).

6.1.2. Access by other competent authorities

380. Intelligence bodies (MIA, NSS, SRC, ACC in this capacity) and investigative authorities (ACC, IC) also have access to an array of databases, such as criminal records, the population register, legal entities register, income tax register, convictions database that are essential for their ML/TF intelligence activities and investigations. In the majority of cases the authorities' access is direct and the information up-to-date. The IC has a database containing persons of interest in criminal cases in order to link investigations. When a new investigation is initiated, the intelligence authorities are informed about the natural persons and entities involved. The SRC (the unit dedicated to combatting tax offences) has also access to information subject to banking confidentiality regarding domestic legal persons.

381. The intelligence bodies do not collect statistics on the level of use of particular databases to perform their functions. The authorities interviewed indicated a standard set of databases is verified in every analysis, followed by a selection of information sources checked according to the needs of a particular case. For example, the SRC in every analysis involving potential ML (whether resulting from a notification from the FMC or stand-alone) verifies the real estate cadastre, data on movable property, the state registry, employment data, tax reports, information on related and dependant persons. Other sources, such as border-crossing data, customs declarations and cash declarations are verified when necessary, depending on the nature of the case. The lack of access to the central bank account register limits intelligence bodies' visibility over financial matters in early stages of investigations, where proceeds of crime/TF could potentially be located in the jurisdiction.

382. Access to bank information for evidence purposes (for example, account statements) requires a court order, which may take a couple of days or more than one attempt to obtain (for details, see IO.7). The SRC has direct access to bank information related to domestic legal persons. In order to identify potential proceeds of crime/TF, intelligence bodies and investigative authorities primarily rely on the FMC to obtain financial information. This is used to establish necessary leads in a case, as the data provided by the FIU cannot be used as evidence in criminal proceeding. The need for access to financial information by competent authorities in the intelligence gathering stage created a strong dependence on the FMC for financial information, especially on the beginning of the period under review.

383. Vulnerabilities identified in IO.5 in relation to identifying the BO of foreign legal persons, and the fact that the State Registry is not fully populated, and the absence of a legal requirement for legal persons to hold a bank account, limit LEAs ability to determine BOs. However, as explained in IO.5, LEAs can also access BO data held by reporting entities (primarily banks, when the legal person has a bank account) mainly through the FMC.

6.2. Production and dissemination of financial intelligence

6.2.1. Production of financial intelligence

384. Armenia has taken significant steps to develop FMC's capacity to produce and disseminate financial intelligence. FIU staff has increased by 30% since the last evaluation and currently consists of 37 persons. In February 2023, a new Strategic Analysis and Supervision Division was established. The unit is divided into five divisions: Analyses (12 employees), Strategic Analysis and Supervision (5 employees), Legal Compliance (5 employees), International Relations (5 employees), and Information Systems Design and Development (6 employees). This increase of resources paired with other activities has resulted in the rising number of FMC spontaneous dissemination to competent authorities and the percentage of ML investigations being triggered by information from the FIU.

385. The FMC has implemented an CMS, which allows for the automated processing, secure storage, and structured handling of the entire volume of information received, analysed, and disseminated by the FMC. Thirteen government agency databases have been integrated into the CMS, accessible through a unified search window to speed up analysis. Nevertheless, the FIU would benefit from more sophisticated IT tools to perform financial analysis, including the visualisation of transactions and network analysis from various data sources and formats. These analytical IT tools would be useful, especially when conducting strategic analysis and operational analysis in more complex cases.

Operational analysis

386. FMC conducts its operational work on the basis of a set of formalized procedures, including inter alia, an operational manual, case analysis guidance and STR prioritisation rules. FMC's cases are primarily triggered on the basis of STRs, but it can also be triggered on the basis of information from foreign FIUs, domestic requests from LEA, open-source intelligence (OSINT) or findings of strategic analysis.

387. The STRs are submitted electronically. Each STR is looked at by an FMC analyst who decides if the STR will constitute the basis for a new case or will be connected to an on-going case. In order to effectively handle incoming reports and requests, each case is manually processed through a prioritization system, which assigns one of four categories: Very High, High, Medium, and Low. The prioritization mechanism identifies which cases should be analysed first by the analysis division. The priority level is proposed by the Head of the Analysis Division and confirmed by the Head of the FIU. The AT looked at the prioritisation criteria and was satisfied that they are relevant, commensurate with the risk and useful for the FIU work[79].

388. Following the prioritisation, every case undergoes operational analysis. The assessment phase of the case can lead either to a comprehensive assessment or a rapid assessment (a simplified analytical procedure) in case of identified as non-essential or low risk STRs. Non-essential STRs can be reports which contain information already available to LEAs, share key characteristics with previously closed cases, have low transaction value or do not connect with other data in FMC databases. Approximately 35% of cases contain reports deemed non-essential and undergo rapid assessment, while the remaining 65% undergo comprehensive assessment. Cases subject to rapid assessment do not end in notifications to other authorities (unless circumstances change) but are used to support other cases of operational and strategic analysis. Cases comprehensively analysed can end either with a dissemination or with the closure of the case.

389. After the completion of the comprehensive assessment the analyst prepares a summary sheet

[79] e.g. the existence of a suspended transaction or business relationship, the underlying criminality – ML/TF, the identification of offences considered the top predicate crimes (ML threats) in Armenia, the value of potential proceeds of crime/TF or the existence of connections to other FIU cases

together with a report addressed to the Head of the FMC. The cases are subject to a 10-point decision matrix based on the probability of occurrence, perception of public danger and potential for funds outflow. When the preliminary score of the proposed hypothesis is more than 6 points, a notification shall be disseminated to competent LEAs. When the preliminary score of the proposed hypothesis (hypotheses) is 4 or 5 points, the names/ titles of subjects of the case can be included in the FMC monitoring list (around contains around 100 natural and legal persons at a given moment), and subject for future review. When the preliminary score of the proposed hypothesis (hypotheses) is 2 or 3 points, no further action shall be taken. The decision on the finalization of the case and eventual dissemination is ultimately taken by the Head of FMC, without any influence from parties outside the FIU. The formalized assessment of each case limits the potential for exerting undue influence on FIU staff.

390. The average time to process a case on the basis of an STR is mostly around 1-2 months and an operational analyst in the FMC normally handles 1-2 STRs per month, which is considered timely. Priority cases can be handled within single days, whereas particularly complex ML cases can take months to analyse and disseminate. Nevertheless, the FIU would benefit from more sophisticated IT tools as explained above.

Table 6.3. Average time of STR turnover

Year	2020	2021	2022	2023	2024
Average number of days to process STR	40 days	42 days	36 days	37 days	35 days

Strategic analysis

391. In February 2023, a new Strategic Analysis and Supervision Division was established within the FMC. The core function of the aforementioned division (5 staff members in total) is to conduct strategic analyses to identify ML/TF-related trends and patterns, assess national risks, and perform ML/TF risk-based supervision over REs that do not have a designated supervisory body in the field of AML/CFT. The FMC staff has attended strategic analysis courses and an in-house strategic intelligence assessment handbook has been developed to support the conduct of such analyses.

392. The FMC undertakes strategic (including thematic) analyses with the aim to a) deepen the understanding of evolving ML/TF risks by competent authorities b) identify unusual patterns of transactions or activities warranting further analysis by intelligence bodies c) produce typologies for reporting entities and d) produce reviews supporting AML/CFT supervisory activities. In the course of the period under review the FMC has carried out strategic analysis on a total of 33 themes (some of them repeatedly on a regular basis). Finalised strategic analyses include, inter alia:

- Strategic analysis on cross border transportation of cash,
- Strategic analysis on money transfers from Armenia to high-risk TF locations,
- Strategic analysis on high-risk customers in the banking sector,
- Typology reports on fraudulent activities, use of third-party intermediaries (money mules), pyramid schemes and drug trafficking,
- Strategic analysis on crypto assets and entities offering such services.
- Analysis of cross-border financial flows and related ML/FT risks connected with chosen jurisdictions.

393. The lack of dedicated analytical software connected with resource constraints (the division devoted to strategic analysis is also responsible for AML/CFT supervision) moderately limits the

possibilities to develop more complex strategic products based on a broader set of data or interact more with other stakeholders. Despite these limitations, the outcomes of strategic analyses have been used inter alia in the NRA, ML typologies and indicators for REs, supervisory inspection plans, and notifications to LEAs.

6.2.2. Dissemination of financial intelligence

394. Throughout the period under review, the number of notifications sent by the FMC to competent authorities have been steadily increasing (from 50 in 2020 to 95 in 2024), which indicates the positive effect of recruiting new analysts, training and efforts aimed at increasing the effectiveness of cooperation with LEAs. The ratio of STRs received by the FMC vs notifications to LEAs based on such reports has risen from 14% in 2020 to 47% in 2024 which highlights the increased capacity of the FMC to share the relevant information with competent authorities coupled with an improvement in the quality of reporting.

Table 6.4. Ratio of all STRs received by the FMC/ STRs used in notifications to LEAs

	2020	2021	2022	2023	2024
All STRs received by the FMC	254	262	254	425	365
STRs used in notifications to LEAs[80]	35	68	58	140	171
Ratio	14%	26%	23%	33%	47%

395. Apart from disclosures on its own initiative, the FMC serves as an important source of information on request for the competent authorities, especially in the context of financial information subject to banking confidentiality requirements. Statistics indicate, that especially in the early years of the period subject to review, the FMC was heavily engaged in providing information to the law enforcement authorities.

Table 6.5 FIU exchange with LEAs

	2020	2021	2022	2023	2024
Notifications from the FMC to LEAs	50	80	66	106	95
Responses from the FMC to LEAs' requests	558	555	407	330	243

6.2.3 FIU financial intelligence supporting needs of competent authorities

396. The FMC is the key source for financial intelligence for Armenian competent authorities, providing information both on its own initiative and on request. FMC notifications have a standardised structure and contain relevant information for further use on analysing ML/TF cases. Feedback collected by the FMC on the use of its spontaneous disseminations suggests, that the majority of the FIU notifications are further used by the competent authorities to trigger or supplement criminal investigations (see core issue 6.4). The FIU disseminates its intelligence products to a wide range of intelligence and investigative bodies.

[80] One notification can contain more than one STR

Table 6.6. FIU notifications to LEAs

LEAs	2020	2021	2022	2023	2024	Total (per LEA)
NSS	37	48	26	38	39	188
MIA	5	20	20	17	20	82
SRC	5	8	8	25	21	67
ACC	0	1	5	10	7	23
IC	1	1	4	13	3	22
GPO	1	2	3	3	5	14
MOJ	1	0	0	0	0	1
Total	50	80	66	106	95	397

397. The recipients of FIU notifications have varied in the period under review due to changes in the framework for conducting ML investigations. Until October 2021, the National Security Service (NSS), apart from its intelligence gathering capacity, held exclusive authority over ML investigations and was the primary recipient of FIU intelligence. In the following period, many authorities (NSS, MIA, SRC, IC) encompassed within their tasks both intelligence and investigative activities. Finally, in January 2023, the Investigative Committee (IC) has taken over as the primary body responsible for ML investigations, with the Anti-corruption Committee (ACC) having competence for ML investigations related to corruption (and – as the only remaining authority – possessing both an intelligence and investigative capacity). The current system is constructed in a manner where (in general) FIU information is first transferred to the intelligence bodies (NSS, MIA, SRC, ACC in this capacity) which enrich the data and (if there is adequate basis) transmit the outcomes in the form of a crime report to the investigative agencies (IC, ACC) to trigger criminal proceedings. The main recipient of FMC notification remains the NSS followed by the MIA (Police).

398. In general, the NSS should receive results of analysis of FT cases and those affecting national security. The SRC would be the recipient of analysis involving potential ML and/or tax evasion and the ACC (in its intelligence function) notifications concerning ML and/or potential corruption. The MIA should be the primary recipient of ML cases involving fraud. Nevertheless, the dissemination process is not fully transparent due to the overarching competence of some of the authorities (primarily the NSS and the MIA) in the field of counteracting money laundering and associated predicate offences.

399. In the beginning of the period under review, the FMC sent the same notification to multiple recipients in case of ML associated with predicate offences spanning across competences of several authorities. This practice was ultimately considered to be less efficient than sending to one authority who would manage further disclosures to other intelligence agencies (for example, in the case of tax evasion – to the SRC). In practice, similar cases (for example, ML associated with fraud or tax evasion) can often have different recipients, depending on the trigger for the analysis. The handling of similar ML cases by different authorities implies that the intelligence authorities need to have a broader range of expertise to effectively analyse disseminations received from the FIU. Limited coordination mechanisms between the intelligence bodies may lead to diminished opportunities for triggering ML investigations (see IO.7).

400. Notifications to the NSS concerning potential TF have been generated on the basis of requests and disclosures from foreign counterparts along with results of the "Regional level operation" (see IO.9).

Table 6.7 Breakdown of FIU notifications to LEAs by underlying offence in the years 2020-2024

ML[81]	TF**	ML + other crime (specify the top 5 offences), including				
		Fraud	Drug trafficking	Corruption	Tax evasion	other crimes
97	5	102	18	68	69	38

401. As indicated earlier, the FIU also notifications to the FSLD on potential breaches of AML/CFT obligations conducted by reporting entities. In particular 27 of these notifications involved the failure to file an STR.

402. The FMC is a vital source of information on request for the law enforcement authorities, in particular the intelligence bodies. Based on the interviews conducted by the AT, it seems the majority of these inquires would concern intelligence gathering activities regarding proceed generating crimes which could potentially lead to ML. 18% of all requests concern ML without reference to any predicate offence. The range of information to be obtained vary from basic data on active bank accounts, account statements, to the provision of information in the FIU database (for example STRs, TTRs) and requests for full FMC analysis. In many cases the FMC contacts reporting entities or foreign counterparts to gather the necessary data. In order to mitigate the number of requests, in cooperation with LEA, in 2020 the FMC developed the Principles for Inquiries, outlining several important elements including the characteristics of admissible and inadmissible inquiries. This led to a gradual decrease in the number of requests made by LEAs to the FMC (see table below). While this is a positive development, the number of requests outnumber by far the FIU notifications on its own initiative which raises concerns regarding the use of FMC resources especially in the context of the absence of more sophisticated analytical tools as explained above.

Table 6.8. Requests by LEAs to the FMC

Requests to FMC	NSS	MIA	ACC	SRC	IC	MoJ	Interpol	MoD	Total
2020	275	74	27	46	134	11	8	0	575
2021	328	209	15	25	32	10	11	0	630
2022	240	105	31	28	19	4	3	0	430
2023	153	70	41	51	13	0	7	5	340
2024	147	36	6	58	15	2	0	1	265

403. In the period under review a total of 49 requests from the NSS concerned potential TF. The requests pertained to various hypotheses related to breaches of public order and extremist activities potentially terrorism related. In all instances, the FMC conducted thorough analyses, including requesting information from REs. No potential links to TF were identified in any of the cases.

6.2.4. Other competent authorities producing financial intelligence (where relevant)

404. Notifications from the FMC to the SRC are analysed by the Investigation and Operational Intelligence Department. Data from the FIU is supplemented with information from inter alia tax databases, the real estate register, employment information, the corporate register which are studied in through operational-intelligence measures to identify signs of tax crimes under the Criminal Code where the damage exceeds 10 million AMD. The SRC uses more than 30 automated analytical risk tools for specific sectors of the economy, operating on the basis of over 500 risk profiles, including

[81] With no predicate attached

those aimed at detecting ML cases.

405. Information received from the FMC becomes the subject of the study of the NSS, within which complex operational-search measures are carried out to verify, substantiate the hypothesis/hypotheses put forward by the FMC. The employees of the NSS, in the course of their work, collect financial intelligence as well as other information relevant to the identification and investigation of ML cases. The employees utilize directly accessible databases, such as databases of the Cadastre Committee, the State Register Agency, etc. and a range of 16 operational intelligence activities).

406. In the case of MIA, once information about a possible ML case has been received, an in-depth analysis is conducted, primarily in the General Department of Criminal Police, to determine its reliability through the implementation of operational-intelligence measures, to assess the available resources and to plan the list, sequence and schedule of necessary measures. Ultimately, a preliminary legal assessment of the alleged crime is performed. In case of existence of reasonable grounds, a report on the alleged offense is sent to the relevant investigative body to discuss the initiation of criminal proceedings.

407. The ACC in its intelligence capacity uses the information available in the relevant electronic databases to verify information provided by the FMC. There are no special mechanisms for using the information contained in the electronic databases to develop operational and strategic analysis. Data provided by the FMC are considered operational data, which are verified by the body carrying out operational-intelligence activities.

408. The outcome of the activities of the intelligence bodies remains a concern for the AT. Limited statistical data is available on the number and nature of disseminations of the MIA, NSS and SRC to the IC and ACC. Interviews with the authorities indicate, that crime reports filed by the intelligence bodies rarely contain a suspicion or hypothesis of money laundering, focusing instead on justified suspicion of the predicate offence. The aforementioned case can be caused by several factors as explained below.

409. One aspect is the expectation that in practice the intelligence bodies would carry out their activities within a relatively short timeframe of a couple of months. This limits the possibility to substantiate a clear ML hypothesis to the investigative authorities. The investigative authorities do not perceive this as a deficiency, as the intelligence body filing the crime report is further involved in the criminal investigation, and ML charges can be added at a larger stage.

410. Another aspect is the resources available to the intelligence bodies. With the exemption of the NSS, none of the aforementioned authorities have designated a specialised unit or subdivision for the analysis of ML cases nor officers specialised in financial matters. While the majority of the staff involved in handling FMC disseminations has received general ML training, the financial aspect remains insufficiently explored at the intelligence level which demonstrate the need for enhanced expertise for the NSS, SRC, MIA and ACC, in order to be able to substantiate the ML hypothesis as a trigger for criminal investigations. Both the MIA and SRC lack dedicated experts in the field of digital and forensic financial examination, although both units have dedicated staff having better financial expertise and understanding of blockchain analysis.

411. The authorities acknowledge a growing trend of using FMC’s financial intelligence data by LEAs to investigate predicate offences, rather than focusing on ML crimes.

6.3. Cooperation and exchange of information/financial intelligence

6.3.1. Co-operation and exchange

412. On the bilateral level, cooperation between the FMC and intelligence bodies, such as the NSS,

SRC or MIA, is facilitated by signed bilateral MoUs which set out the specific roles and needs of parties as well as a more detailed framework for cooperation on specified matters, including exchange of information, organization of trainings, setup of bilateral discussions or meetings and the development of handbooks and typologies. These include arrangements to hold bilateral or multilateral discussions on potential cases or hypotheses of ML – within 5 working days and potential cases or hypotheses of TF or PF – without delay and in any case not later than within 1 working day. This power is used regularly by the FIU and inquiry bodies in top priority cases. While no formal cooperation mechanism is in place, meetings with the supervisors are initiated in the context of cases involving reporting entities and in the context of developing and providing typologies to the financial sector and non-financial sector.

413. The authorities use a dedicated Financial Intelligence Data Exchange Platform – a secure communication system specifically designed to support protected data exchange. This system ensures that sensitive information is transmitted in a secure, encrypted environment, accessible only to designated officials within authorized institutions.

414. In key ML/TF cases, where enhanced cooperation between REs, the FMC and LEAs are necessary to ensure effective analysis, the FIU can set up task forces and partnerships. In particular, such cooperation is exploited in particular grand corruption cases. This is a positive outcome, which allows to both speed up the analysis and facilitate broader collection of information.

Box 6.1. FIU – LEA cooperation on ML and corruption case

A PEP, with the assistance of others, received a particularly large bribe of 14 million USD in exchange for taking actions within the scope of his official powers to benefit a Resident Entrepreneur by facilitating the granting and extension of mining licenses.

One part of the bribe was given in cash, while the other part was transferred through foreign bank accounts belonging to other individuals and was subsequently laundered.

The scheme involved inter alia: a UAE Company which entered into an agreement with the Resident Entrepreneur to purchase a mining company in Armenia for 40 million USD; a close associate of the PEP and a prominent entrepreneur in Armenia; a BVI Company with a bank account in Switzerland beneficially owned by the associate; an Armenian Company - alcohol factory engaged in legitimate business activities in Armenia. Its beneficial owner is the associate of the PEP; a series of individuals affiliated with the PEP who conducted transactions based on his instructions.

Among other extensive investigative activities, it was possible to uncover the entire transaction scheme and identify the real beneficial owners through a parallel financial investigation, which included intelligence provided by the FMC.

Banking information related to the UAE and Switzerland was obtained from the respective countries within the framework of mutual legal assistance and was subsequently used as evidence in the course of the investigation. During the preliminary investigation, the bank accounts of the persons, movable and immovable property actually belonging to them or available in their names were frozen in the Republic of Armenia. In 2023, the case was submitted to the court and currently in the stage of main court hearings.

6.3.2 Security and confidentiality

415. The FMC's network operates as a secure segment within the CBA network, benefiting from perimeter protections including firewalls located at the CBA network boundary. Although structurally part of the CBA, the FMC operates with a high degree of technical independence. It maintains its own dedicated IT division and infrastructure to support its functions. To further strengthen its internal control environment, the FMC established a dedicated IT Security Officer position in 2023. Technical

independence is maintained internally, while cybersecurity oversight is provided in cooperation with the CBA's cybersecurity unit. The FMC's servers are completely separated from the CBA's general IT infrastructure. Information that is maintained on servers, databases and applications is only accessible to FMC's designated staff.

416. All data exchanged between the FMC and its domestic or international counterparts is transmitted through secure, encrypted channels to preserve confidentiality and data integrity. At the international level, information exchanged with foreign counterparts is secured via Egmont Secure Web and the CIS FIU network.

417. FMC analysts regularly request and receive information from FIs on a daily basis via secure channel (CBAnet). All sensitive data that is transferred between FMC and REs is encrypted using to prevent unauthorized access.

6.4. Using information/financial intelligence

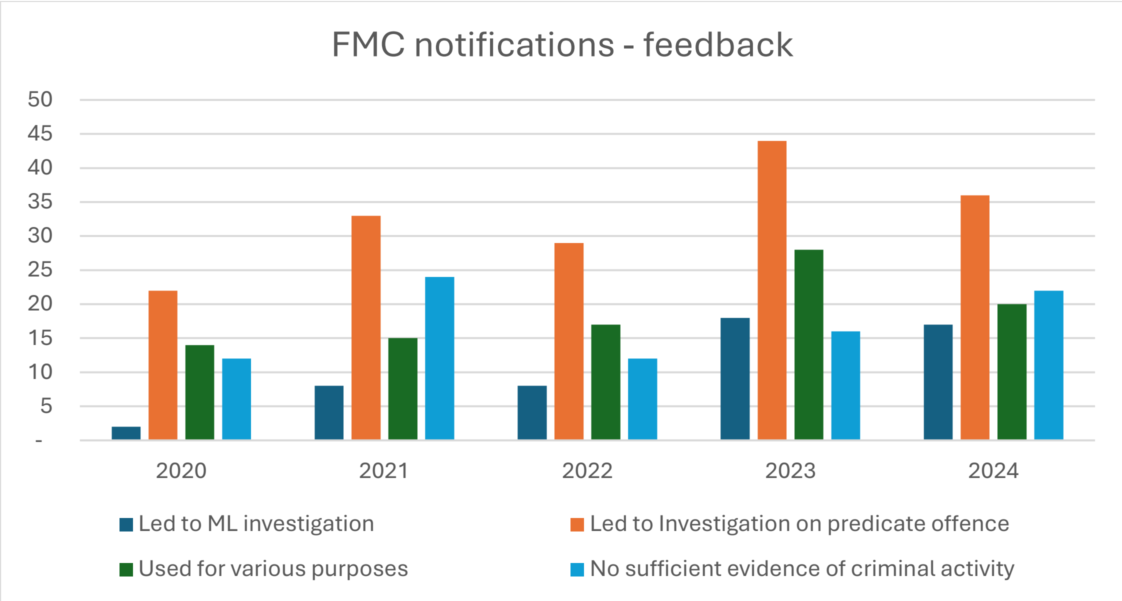
6.4.1. Using information / financial intelligence for investigations and developing evidence

418. Feedback collected by the FMC on the use of its spontaneous disseminations suggests, that the majority of its notifications have led to opening an investigation or added value to existing cases in various ways [82].On a less positive note, the majority of FMC notifications were not use in ML cases but in predicate offences investigations. While the FMC routinely highlights ML hypothesis in their disseminations, the investigative bodies often concentrate on the predicates and do not follow the ML aspect. As explained under 6.2, this may be due to several factors not directly related to the quality of FMC disseminations.

419. The FIU uses a feedback system to monitor the use of its spontaneous disseminations with a view to improve its quality. This includes cases which did not lead to criminal investigations. One of the results of feedback received from LEAs on card-fraud investigations, was the decision to widen the scope of analysis of the FMC to include more detailed information on the victims of crimes.

[82] Use for various purposes in connection to existing criminal cases, such as to support the seizure of property, the submission of MLA requests, the conduct of parallel financial investigations, the identification of illicit assets, the development of evidentiary material, etc.

Graph 6.1. Outcomes of the FMC notifications



420. Although the FMC information is considered essential for the work of the LEAs, in the period under review, the FIU did not play a key role as the trigger for ML investigations. This trend started to change in the recent years, due to more focus and resources being put in the increase of the number of disseminations along with simultaneous efforts to decrease the number of LEAs requests for banking confidentiality data. The FIU recently (2024) became one of the key triggers of information allowing to initiate ML investigations at a later stage.

Table 6.8. ML investigations by source

Source	2020	2021	2022	2023	2024	
Parallel financial investigations	20	7	13	50	38	
FIU disseminations	1	1	3	13	30	
Domestic intelligence	0	0	3	8	11	
Open-source information	0	1	1	1	0	
MLA	0	0	0	0	0	
Foreign intelligence	0	0	0	0	0	
Other sources	0	3	6	8	8	
Total	21	12	26	80	87	

421. In the majority of cases where ML investigations are initiated, the FIU was involved, primarily as a source of information on request. While shortcomings concerning the level of reporting from reporting entities to the FMC and further activities of LEAs may affect its ability to be able to trigger ML investigations, FMC data still remains a key source of data for LEAs to develop leads on financial flows.

Table 6.9. FMC involvement in initiated ML investigations

	2020	2021	2022	2023	2024	Total
Initiated ML criminal proceedings	21	12	26	80	87	226
ML criminal proceedings where the FMC filed disseminations*	2	1	5	16	33	57
ML criminal proceedings where the FIU provided information on request of LEAs	18	9	12	47	24	110

**The numbers in this row are different from those under Table 6.8 as a single dissemination may lead to more than one ML investigation*

6.4.2. Using information / financial intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

422. The FMC supports LEAs by providing the relevant financial analysis on transactions and bank accounts allowing to identify proceeds. Case studies presented, especially those concerning laundering the proceeds of corruption and embezzlement by public officials, demonstrate the ability of intelligence agencies and investigative authorities to use financial intelligence to identify and trace criminal proceeds. Each intelligence and investigative body is responsible to identify and trace criminal property and prepare sufficient evidence in their cases, with a view to confiscation. However, the results obtained so far are not convincing in that asset identification is systematically pursued in pre-trial investigations. The FIU has demonstrated the capability to apply suspension mechanisms on different occasions (see IO.8).

Chapter 7. Money Laundering Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Since the last evaluation, Armenia's legal and institutional framework for identifying, investigating and prosecuting ML has undergone important changes. In 2021, new Criminal and Criminal Procedure Codes were adopted, revising the responsibilities of the relevant LEAs involved in intelligence-gathering and investigations into ML and associated predicate offences.

b) ML investigations are mostly triggered from investigations into predicate offences. The current institutional set-up, with competences primarily focused on predicate crimes, results in a predominantly predicate-offence-driven system. The number of ML investigations originating from disseminated FIU intelligence has risen, especially in the last two years. However, other potential sources for ML cases such as MLA requests, foreign intelligence and cash seizures are underutilized. Overall, there is a strong emphasis on the domestic component of predicate offences, with limited consideration given to ML with foreign or transnational organised crime nexus, which impacts the type and scale of cases pursued.

c) An increasing trend in the number of ML investigations and prosecutions in the last two years has been observed, corresponding largely with the identified ML threats. However, the number and the characteristics of these are still not in line with the overall level of ML risk, considering the limited risk understanding of ML relating to foreign predicated or transnational crime (as described under IO1). Corruption-related ML investigations are predominant, reflecting recent reforms. ML investigations linked with other high-risk predicate offences, such as tax evasion, fraud and drug trafficking, are fewer and not aligned with the volume of those crimes. While prosecutions involving corruption and drug trafficking ML are following the investigations' trend, the prosecutions for tax-related ML are very limited. The focus remains on self-laundering cases, while third-party and autonomous ML cases are not systematically pursued.

d) The number of convictions remains modest and limited to self-laundering and small-scale cases associated with fraud. Although there are few examples of complex and large-scale ML investigations and prosecutions, no conviction has featured such profile. This may be a result of several factors: the limited use of financial intelligence by LEAs at the intelligence gathering phase; the absence of an integrated platform for information exchange among the various inquiry and investigative bodies; the limited scope of LEAs powers to access banking information for evidentiary purposes; the inability to initiate investigations against legal persons; the higher evidentiary standard and restrictive interpretation for certain elements of ML offence; or the significant resource constraints faced by the courts.

e) Criminal sanctions imposed are neither effective nor dissuasive. No alternative criminal justice measures have been implemented to address ML when it was impossible for justifiable reasons to achieve a conviction.

Key Recommended Actions (KRA)

a) Armenia should take measures to actively pursue the investigation and prosecution of ML, particularly of complex third-party and autonomous ML cases, and ensure that all relevant sources are fully utilised for potential ML identification, with appropriate consideration to be given to all potential foreign or transnational links. The country should take measures to ensure that convictions are secured in all types of ML cases and that the sanctions applied are effective, proportionate and dissuasive.

b) Armenia should ensure that the interpretation and understanding of ML offence by Courts in relation to the purposive element of certain acts of ML, does not impede prosecution of ML cases in line with international standards.

c) The authorities should review the investigative bodies' access to financial information for evidentiary purposes, ensuring that they can obtain all information necessary for investigations and prosecutions of ML and associated predicate offences, even in the absence of a direct link to or control by the suspect or the accused, in order to facilitate the identification of the extent of criminal networks and/or the scale of criminality, in particular in third-party or autonomous ML cases.

Other Recommended Actions

d) Authorities should develop an integrated platform for information exchange among the inquiry and investigative bodies, as set out in the AC Strategy.

e) Armenia should assess the reasons for the absence of investigations into legal persons and develop formal guidelines on domestic requirements and international good practices to address potential impediments (e.g. the restrictive understanding by LEAs on the requirements of a prior conviction of a natural person).

f) Additional resources (*i.a.* human, material, technological) should be allocated to courts to manage the increasing workload and ensure the timely and effective adjudication of the ML cases.

g) LEAs should further develop their tracing skills and acquire appropriate IT tools for virtual asset–related crimes to effectively address emerging risks in this area.

Overall conclusion on IO.7

Armenia has made efforts in recent years to enhance the effectiveness of ML investigations and prosecutions through significant changes to the relevant legal and institutional framework. This includes positive progress in anti-corruption reforms, particularly in terms of policy development and strengthening the anti-corruption institutional framework. These developments have contributed to an increase in ML investigations and prosecutions over the last two years and positively impacted the pursuit of corruption-related ML cases, including high-profile ones, which account for the majority of ML investigations. ML investigations and prosecutions feature the main identified threats. However, the number and the characteristics of these are still not fully in line with the overall level of ML risk. There is insufficient proactive use of both domestic and foreign intelligence, and cooperation between intelligence and investigative bodies remains driven on an ad hoc basis.

Stand-alone and third-party ML cases remain rare, with the investigations continuing to be predominantly focused on self-laundering linked to domestic predicates. No investigations have been initiated against legal persons, despite indications that legal persons are frequently involved in ML and associated offences. Prosecutions are following the investigations trend but are often prolonged, hindered by evidentiary challenges and procedural delays.

There are few examples of complex, internationally linked ML cases for which the authorities are commended. However, no convictions reflect such profile. The seven convictions achieved during the period under review involve small-scale self-laundering cases associated with fraud. This is not in line with the international standards on effectiveness, or with the country's risk profile. Armenia has not pursued alternative criminal measures. Nevertheless, an example was provided in which civil confiscation measures were applied, resulting in criminal property being transferred to the state based on a settlement agreement within civil proceeding.

The country has acknowledged these deficiencies and has incorporated relevant actions in its 2025-2028 AML/CFT/CPF National Strategy to address them.

Armenia is rated as having a low level of effectiveness for IO.7.

7.1. ML activity identified and investigated

423. Following the adoption of a new CPC in 2021, and its subsequent amendments, organisational reforms have reshaped the intelligence gathering and investigative system in Armenia. Various authorities have taken responsibility for investigating ML at different stages during the period under review. From 2015 until October 2021, the National Security Service (NSS) held exclusive authority over ML investigations. As of January 2023, the Investigative Committee (IC) has taken over as the primary body responsible for ML investigations, with the Anti-corruption Committee (ACC) having competence for ML investigations related to corruption. The National Security Service (NSS) Ministry of Internal Affairs (MIA) and the State Revenue Committee (SRC) were divested of investigative powers and now function primarily as intelligence-gathering bodies. The results of the intelligence gathering conducted by the three bodies are referred to the IC and, where appropriate, may also be referred to the ACC.

424. As a result of organisational reforms, part of the existing LEAs' staff prior to 2021 was reassigned to the newly establish investigative bodies (the IC and the ACC) and additional positions were created. Investigators within the IC and ACC are supported by specialised experts in financial forensic examinations (eight within the IC and four within the ACC), as well as digital forensic experts (6 within the IC and 1 within the ACC). None of the intelligence bodies have specialised experts in financial matters (see IO6). When necessary, additional expertise (eleven financial experts) can be drawn by the IC and ACC from laboratories under the MoJ and the National Academy of Science. Efforts to address remaining vacancies are undergoing. Apart from the SRC, other inquiry and investigative bodies seek to strengthen their capacity thorough the recruitment of additional staff, including investigators, financial experts and IT specialists. The MIA is also planning to create a specialised laboratory (CyberLaB) for digital and crypto-related forensics.

425. The intelligence and investigative bodies have trained staff to investigate ML. None have specialised staff or dedicated units focused exclusively on ML. The units responsible for intelligence gathering or investigating the predicate crimes also deal with associated ML. Case allocation is based on the experience and skills of individual analyst or investigator.

ML activity identified

426. Most ML activity is identified in the context of investigations into predicate offences (see Table 7.1.). An increase in cases where ML was identified on the basis of the FMC dissemination has been observed only in last two years of the assessed period. This is a positive trend. There are no cases in which ML investigations originated from information related to cash seizures, incoming MLA requests, or foreign intelligence. While the authorities consider this to be consistent with the country's risk profile, concerns remain as to whether the external threats and foreign nexus elements are being fully taken into account (see IO.1, IO.2 and IO.6).

Table 7.1. ML investigations by source

Source	2020	2021	2022	2023	2024
Parallel financial investigations	20	7	13	50	38
FIU disseminations	1	1	3	13	30
Domestic intelligence	0	0	3	8	11
Open-source information	0	1	1	1	0
MLA	0	0	0	0	0
Foreign intelligence	0	0	0	0	0
Other sources	0	3	6	8	8

427. Based on interviews with LEAs and presented ML cases, the AT observed a system that is generally "predicate-offence-driven". This may stem from the existing institutional set-up, in which intelligence-gathering and investigative bodies have competences focused on certain predicate crimes. At the same time, the AT noted overlapping responsibilities among intelligence bodies. For example, while the ACC and the Tax Department of the SRC have more clearly defined thematic areas (corruption and tax evasion), there are still cases where large-scale tax evasion are handled by other authorities (e.g. NSS or MIA). Similarly, drug-related offences may be handled by MIA, NSS or SRC.

428. There is no integrated database or platform for systematic information exchange among intelligence and investigative bodies. While cases can be discussed in Inter-Agency Committee meetings or ad-hoc as needed, there is no formal intelligence-sharing mechanisms among LEAs. Clarifying the division of responsibilities and establishing an integrated platform to facilitate information exchange between the intelligence units, investigative and prosecutorial bodies, as envisaged by the AC 2023-2026 Strategy, would be beneficial. Without such measures, this fragmentation may lead to diminished opportunities in detecting ML.

429. The IC mainly relies on the intelligence reports submitted by NSS, MIA, SRC and the ACC (in corruption-related cases). The ACC largely relies on its own intelligence gathering activities - approximately 50-60% of ACC investigations are initiated through its own intelligence. Most ML investigations are initiated only after certain investigative actions have already been carried out in relation to the predicate offence, which may indicate that ML is being overlooked at the earlier stages. Neither the IC nor the ACC could recall a case in which ML was included in the initial report submitted by intelligence bodies. No statistics are maintained to illustrate at which stage the ML component is most frequently added. In most complex or large-scale cases presented to the AT, ML charges were added by the GPO alongside the predicate offence, rather than by the investigative bodies.

ML investigations

430. Over the reporting period, a total of 226 ML investigations were initiated, all involving natural persons. A significant increase is noticed in the last two years of the assessed period (2023-2024)

indicating that recent reforms impact the system positively (see Table 7.2.). Overall, compared with the previous reporting period (2010-2014), during which 53 ML investigations were initiated, this reflects a positive trend.

431. Almost half of ML investigations are in relation to corruption (see Table 7.3). In some case, complex or large-scale cases, joint investigative groups may be established. Three examples have been provided in relation to jointly investigations by the IC and ACC.

432. ML investigations have also been initiated in connection with drug trafficking, tax evasion and fraud, which is consistent with the main ML threats identified by the country. The number of ML investigations connected to high-risk predicate offences (Table 7.3) appears to be relatively low when compared to the total number of investigations into these high-risk offences—particularly for fraud, drug trafficking, and tax evasion (Table 7.4). Authorities attribute this difference to the presence of "petty crimes" that are not having necessarily a ML component. However, while this explanation is acknowledged, it does not fully account for the observed gap. The AT has also noticed a strong emphasis on the domestic component of predicate offences, with limited consideration given to foreign or transnational organised crime nexus. This impacts the type and scale of cases pursued.

433. Since 2022, a total of 16 investigations were initiated in autonomous ML cases, which represents an improvement compared with the previous reporting period.

Table 7.2. ML Investigations 2020–2024

Year	Cases	Natural persons	Legal persons
2020	21	19	0
2021	12	20	0
2022	26	23	0
2023	80	68	0
2024	87	58	0

Table 7.3. ML investigations related to high-risk predicated offences

Offence	2020	2021	2022	2023	2024	Total
Fraud	1	1	2	5	4	13
Cyber fraud	-	3	2	5	21	31
Embezzlement	1	2	3	5	4	15
Drug trafficking	2	4	1	14	10	31
Corruption	14	6	9	34	30	93
Tax crime	2	-	1	4	6	13
Stand-alone ML	-	-	2	7	7	16

Table 7.4. Investigations into high-risk predicate offences

Offence	2020	2021	2022	2023	2024	Total
Fraud	1713	1861	1997	2497	3060	11128
Drug trafficking	791	981	1450	3060	2357	8639
Corruption	1008	934	1022	1848	961	5773
Tax crime	164	275	579	234	207	1459

434. As mentioned above, almost half of the ML investigations are in relation to corruption. Armenia has made positive progress in anti-corruption reforms[83], including through policy development, considerable legislative advancements, the enforcement of corruption offences, and the strengthening of the anti-corruption institutional framework, notably by the establishment of specialised institutions

[83] Armenia: Fifth round of anti-corruption monitoring follow-up report, OECD (2025).

such as the ACC, a specialised department within the GPO dealing with cases from the ACC, and the Anti-Corruption Court. These developments have positively impacted the pursuit of ML cases linked to corruption. Most ML investigations initiated by the ACC remain originating from parallel financial investigations. Case examples demonstrate authority's ability to investigate ML cases in relation to corruption, including high-profile cases (see cases examples in Box 7.1 and 7.2).

Box 7.1. ML associated with corruption

The criminal investigation of corruption was initiated in 2021 on the basis of a citizen's complaint. The ML investigation was initiated following the preliminary investigation into corruption.

The former Armenian Minister of Environmental Protection, with help from associates, accepted a particularly large USD 14 million bribe to facilitate obtaining mining licenses for a Resident Entrepreneur. Of this, USD 6 million was handed over in cash, while USD 8 million was routed through foreign bank accounts and laundered.

Key elements of the scheme included:

- A UAE company buying an Armenian mining company for USD 40 million.
- The bribe was funnelled via companies in the BVI and Armenia, as well as bank accounts in Switzerland and the UAE linked to the Minister's associates.
- Individuals affiliated with the Minister carried out instructions to disguise the bribe as legitimate business transactions.

Through a parallel financial investigation, which included intelligence provided by the FMC, it was possible to uncover the entire transaction scheme and identify the real beneficial owners. Banking information from UAE and Switzerland was obtained within the framework of mutual legal assistance and was subsequently used as evidence in the course of the investigation. During the preliminary investigation, the bank accounts of the involved persons, the movable and immovable property belonging to them or available in their names were seized in the Republic of Armenia. Although no details were provided on the value of seized property, it is known that the value of assets subject to possible confiscation is USD 14 million. In 2023, the case was submitted to the court and currently in the stage of main court hearings.

435. Although the number of ML cases linked to tax crimes remains relatively low, tax evasion represented the primary predicate offence which triggered the investigation and prosecution of the most complex ML case in Armenia, involving tax evasion and high-profile corruption (see Box 7.2.). The SRC provided examples of cases involving transnational tax evasion schemes and potential ML, linked to companies registered abroad - Cyprus, the United Kingdom, and Northern Ireland. In one case, a domestic company transferred substantial funds to a Cypriot entity under a false trademark sale to evade taxes. Another case involved false invoicing in the petroleum sector by a domestic company, resulting in USD 14 million in cash withdrawals. According to authorities, these cases are currently under investigation by the IC, and the outcomes of the investigations are to be seen later.

Box 7.2. Case study - ML associated with tax evasion and corruption

This investigation concerns several serious offences, including money laundering, tax evasion (approx. USD 1 million), abuse of official authority, forgery, and illegal participation in entrepreneurial activity. The case originated from a parallel financial investigation in July 2018, initially focused on tax evasion, but subsequently expanded to uncover a network of corruption, money laundering, and other related crimes. The principle criminal case encompasses more than 20 additional cases and 76 distinct episodes.

A PEP was identified as the ultimate beneficial owner of several legal entities used to carry out illicit financial transactions. Through mutual legal assistance requests sent to multiple countries (Italy, Latvia, Switzerland, BVI, Lithuania, Cyprus, UAE, etc.), authorities traced and identified criminal assets and activities organized and orchestrated by the PEP.

A key component involved the sale in 2010 of a state-owned entity at a price well below market value – USD 1 million. The acquiring company transferred a total of USD 4.5 million to bank accounts in Armenia, including state budget and the accounts of the acquired entity, from its bank accounts in Latvia and mostly in Switzerland.

Funds related to this sale, subsequent investments and resale, displayed suspicious patterns: use of multiple Armenian and foreign companies controlled by the PEP and his associates, rapid transfers among various accounts with no clear business purpose, large cash withdrawals, and no real change in ultimate ownership after the resale.

Between 2011 and 2019, further multiple fund transfers were made by foreign and domestic legal entities controlled by the PEP, his associates, and family members to acquire shares in major Armenian companies (approximatively USD 8 million), or to make payments to major Armenian companies for various purposes (approximatively USD 50 million for various services, advanced payments, etc.). These activities indicated ongoing efforts to obfuscate and commingle illicit funds. The shares were repeatedly moved between individuals or companies owned, controlled or associated with the PEP through fraudulent agreements. In some cases, funds were withdrawn in cash from the accounts of legal entities and then deposited into the accounts of other entities or individuals associated with the PEP, with the aim of further investment.

The estimated value of seized assets in Armenia and abroad is approximatively USD 350 million, including foreign bank accounts and shareholdings in foreign legal entities. Part of the criminally obtained property was voluntarily compensated by the accused persons. The investigation resulted in separation of the proceedings. Out of the 50 individuals subject to the investigations, 13 have been indicted. The investigations into the remaining individuals are ongoing. No details on whether all 13 indictments relate to ML or to other predicate offences or whether the ongoing investigations concern ML in all cases.

436. Fraud, in particular cyberfraud, is one of the emerging threats in the country. Many of the presented cases related to fraud, as well as drug-related offences, indicate that proceeds are laundered by transfers to crypto-wallets, followed by conversion into fiat currency, cash withdrawals or transfers via payment systems (see cases studies described in Box 7.3.). The MIA's Cybercrime Unit has developed expertise in tracing and analysing cryptocurrencies, supported by modern analytical tools. Example of cases were given where MIA’s experts successfully traced virtual assets linked to illicit funds. Nevertheless, intelligence and investigative activities in this area are perceived as challenging, due to its complexity and the fact that they rely cooperative relationships with virtual asset service providers which are not yet licenced.

Box 7.3.

Case study 1 - ML associated with cyberfraud

The ML investigation was initiated as a result of the investigation into the predicate crime – computer fraud, illegal entrepreneurial activity and the establishment and management of a criminal organisation.

A criminal organization led by one individual and involving about 30 members collaborated with foreign nationals to commit computer fraud and money laundering. They operated from rented offices in Armenia, contacting victims abroad and luring them into fake investment opportunities via fraudulent websites, resulting in financial losses. The estimated value of damages is USD 26 400.

To hide their crimes, the group registered a number of companies in Armenia pretending to offer legitimate services like employment and software development. These companies were fronts to disguise the source of illicit funds. The illicit funds were also laundered through transfers to e-wallets, which were further moved to cryptocurrency wallets.

During the investigation, with the assistance provided by the FIU, banking records for over 15 individuals and legal entities were obtained. Assets equivalent to approximatively 300 000 USD were seized/frozen in Armenia. The information obtained from European countries, notably Germany, facilitated the identification of similar criminal organizations and a total of 6 offices located in Armenia of similar criminal organisations were dismantled.

Three criminal leaders were identified on which an international search was subsequently initiated. No indictments have been issued yet against the members of the criminal organisations.

Case study 2 - ML associated with drug trafficking

The ML investigation was initiated as a result of a preliminary investigation concerning narcotic drug sales.

Person X organised and operated multiple Telegram-based shop platforms for the illegal sale of large quantities of narcotic drugs. He recruited numerous individuals into a well-structured criminal organization, assigning specific roles to each participant such as cultivation, production, transportation, sale of drugs, and money laundering. During 2021-2022, the criminal group used cryptocurrency accounts, particularly on the Binance platform, to receive and launder large sums (e.g., USD 780,000 of which USD 700,000 was transferred and exchanged) before distributing proceeds in cash among members. In some cases, the cryptocurrency was exchanged and provided to the members of the criminal organisations through both cash and electronic payments.

The founder of the criminal organisation and other 9 individuals have been indicted (no details on whether all 10 indictments relate to ML). The case is currently pending before the court. The founder was located abroad based on an international search and arrested. Extradition proceedings are currently under way. The investigation was suspended in relation to one person based on a settlement agreement. Movable and immovable property belonging to three individuals was seized, although no details regarding the value of the seized property are available.

437. According to the authorities, parallel financial investigations are routinely conducted. It was confirmed during on-site interviews that such investigations are mandatory in each criminal case. This may impact the prioritisation of available resources and cases based on the threat or scale.

438. Another concern relates to the scope and depth of the financial investigations conducted. As mentioned above, there is an important emphasis on the domestic nature of the offences, with limited focus on the potential links to foreign elements or transnational organised crime. A case example discussed during on-site related to the seizure of large quantity of cocaine (~1 tone) imported from Ecuador via Panama, Italy and Georgia by an Armenian company whose owner and BO was a domestic PEP, revealed that the parallel investigative actions and MLA requests did not uncover any illicit proceeds or illicit conduct in relation with the involved company. Similarly, no tangible results were reported in another case discussed involving the seizure of massive quantity of cocaine (~2.7 tons) in Italy, intended to be imported into Armenia, nor in other cases of similar nature involving transnational elements.

439. Obtaining relevant financial intelligence is essential for effective financial investigations. In practice, intelligence and investigative authorities rely primarily on the FMC to obtain various types of financial intelligence, including data on active bank accounts, information available in the FMC's database, information from reporting entities or foreign counterparts. A gradual decrease in the number of such requests, as indicated in Table 7.5, is attributed to the FMC's efforts to streamline such inquiries. While the FMC's support is important at the intelligence-gathering stage for establishing necessary leads, and the LEAs are satisfied with its quality, it can be observed that most of the inquiries relate to predicate offences rather than ML (see IO6).

Table 7.5. Requests made by LEAs to the FMC

Year	Total number of requests by LEAs
2020	575
2021	630
2022	430
2023	340
2024	265

440. FMC intelligence cannot be used as evidence in criminal proceeding. For evidentiary purposes financial information (banking or related information) needs to be obtained through seizure measures based on a court decision. Based on interviews, there appears to be no uniform practice, and similar requests to access information under the same circumstances may be assessed differently by judges. On a positive note, the investigators reported that courts' decisions are generally issued swiftly and there is always a possibility to appeal in case of refusal. There are no comprehensive statistics on the number of requests or court approval rates; according to the IC, approximatively 9.7% of such requests are rejected. When approved, the process to access banking and related information may take up to three to four days. These factors may impact the timeliness of access to necessary financial evidence.

441. One of the findings of the previous assessment concerned the complex legislative provisions which inhibited LEA's ability to obtain the necessary financial evidence. The provision applied only to persons who were formally suspects or accused, and the 2015 MER recommended expanding these powers. Amendments adopted by Parliament in 2020 to broaden access to any financial information essential for investigations, were subject to review by the Constitutional Court, which found them not compliant with the constitutional principles. As a compromise solution, the new provisions of the CPC broadened LEAs' powers, allowing access to banking and related information not only in relation to suspects or accused persons, but also in relation to their associates (where a direct connection exist), as well to legal persons managed or controlled by them. According to the NRA, LEAs have positively assessed the new provisions. While this is acknowledged, the scope of these powers remains limited and does not ensure the access to *all necessary* information necessary for the investigation of a ML or predicate offence (see R.31). Even if in practice, as explained by the authorities, some judges have been willing to interpret the legal framework flexibly, it remains open to different interpretation and legal challenges.

442. Beneficial ownership information is predominantly obtained by LEAs from the reporting entities. In such cases, obtaining BO data is subject to the same rules regulating the access to banking and related information, and the same limitations apply. This undermines the investigative bodies' ability to efficiently determine the extent of criminal networks or the scale of criminality, in particular in third-party and autonomous ML cases.

443. As confirmed during the on-site interviews, investigations are often delayed due to limited forensic and commodity expertise, as well as delays in responses to MLA requests. Some ongoing court cases presented to the AT date back for more than six years. The country has acknowledged this deficiency and as outlined in the strategic steps (5.1 & 5.2) of the National AML/CFT/CPF Strategy, efforts are being made to reduce the time required for expert examinations and improve the training in MLA requests.

444. No investigations have been initiated against legal persons for ML or predicate offences. This is despite corporate liability provisions being in force since 2023. Although not a legal requirement, authorities indicated that legal person's criminal liability depends on a prior conviction of a natural person. According to the explanations provided on-site, any investigation of a legal person can be carried out only after the conviction of the natural person. This raises concerns regarding LEAs' ability to investigate ML in relation to legal persons. This is particularly relevant considering that the provided case examples and typologies associated with the main ML threats frequently indicate the involvement of legal persons.

7.2. Prosecuting and convicting different types of ML activity[84]

445. Armenian legal system allows for pursuing all types of ML. During the assessment period, most prosecutions related to self-laundering, involving 124 individuals, with proceedings against 116 individuals remaining ongoing[85]. As noted in the previous assessment, the authorities appear to continue focusing on self-laundering cases involving mainly domestic predicate crimes. Only one prosecution involved a foreign predicate crime. There was a slight increase in third-party ML prosecutions in 2023, however, the overall number remains low, with very few prosecutions for autonomous ML cases. On the positive note, there was a noticeable increase, approximately fivefold, in the number of self-laundering prosecutions in 2023 and 2024. The authorities were also able to demonstrate few examples of prosecutions (resulted with indictment) in large-scale self-laundering and third-party ML cases (see case examples described under section 7.1.). On the other hand, there have been no prosecutions of legal persons, despite evidence of their involvement in the cases presented to the AT, including complex or large-scale ML cases.

Table 7.6. Types of ML prosecutions and convictions (persons)

Type of ML	2020	2021	2022	2023	2024	Total
Self-laundering						
Prosecutions, of which:	**2**	**10**	**12**	**51**	**49**	**124**
- On-going	**1**	**10**	**9**	**48**	**48**	**116**
- Discounted (statute of limitations or death)	**0**	**0**	**1**	**1**	**0**	**2**
- Acquittals	**0**	**0**	**0**	**2**	**1**	**3**
Convictions	**4**	**0**	**0**	**3**	**1**	**8**
Third party ML						
Prosecutions, of which:	**0**	**8**	**2**	**16**	**5**	**31**
- On-going	**0**	**5**	**2**	**14**	**5**	**26**
- Discounted (statute of limitations or death)	**0**	**3**	**0**	**2**	**0**	**5**
- Acquittals	**0**	**0**	**0**	**0**	**0**	**0**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Standalone ML						
Prosecutions, of which:	**0**	**2**	**0**	**5**	**2**	**9**
- On-going	**0**	**2**	**0**	**5**	**2**	**9**
- Discounted (statute of limitations or death)	**0**	**0**	**0**	**0**	**0**	**0**
- Acquittals	**0**	**0**	**0**	**0**	**0**	**0**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Foreign predicate crime ML						
Prosecutions, of which:	**0**	**0**	**0**	**1**	**0**	**1**
- On-going	**0**	**0**	**0**	**1**	**0**	**1**
- Discounted (statute of limitations or death)	**0**	**0**	**0**	**0**	**0**	**0**
- Acquittals	**0**	**0**	**0**	**0**	**0**	**0**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**

446. The authorities did not provide a specific reasoning for the predominant focus on self-laundering cases and the limited number of autonomous ML prosecutions. There is a common understanding among the authorities that a prior conviction is not required to pursue a ML case, and that the intent and knowledge necessary to prove ML can be inferred from objective factual circumstances. Consequently, the results may reflect the priorities of the investigative and prosecutorial authorities (see also the analysis under section 7.1 in relation to the institutional set-up of the inquiry and investigative bodies). On the other hand, the authorities referred to the difficulty in proving the intent to launder illicit proceeds, as one of the challenges. The latter may suggest a higher evidentiary standard. This is particularly relevant for ML offence committed through the "acquisition, possession

[84] *See Methodology, IO.7, Note to Assessors 2 and related footnotes*

[85] The statistics presented in Table 7.6. are based on the number of individuals charged, thus the actual number of ML prosecutions may be lower.

or use of property”. These cases require proof of the intent to launder the property, which goes beyond the requirement established under the international standard (see R.3).

447. Most ML prosecutions are pursued jointly with predicate crimes. These primarily involve fraud, drug trafficking and corruption, including cases related to organised crime (Table 7.7). This is largely consistent with the identified main ML threats, with the exception of tax evasion, in relation to which there has been only one prosecution. However, the results are still not fully in line with the overall level of ML risks, both in terms of number or characteristics, given the relative low number of prosecutions compared with the level of predicate criminality and the limited understanding of risks related to foreign threats or transnational crime (see IO1).

Table 7.7. ML prosecutions and convictions related to high-risk predicate offences

ML associated with	2020	2021	2022	2023	2024	Total
Fraud						
Cases associated with the offence	**1**	**3**	**4**	**5**	**6**	**19**
Prosecuted persons	**1**	**9**	**5**	**6**	**9**	**30**
Cases where conviction was reached	**2**	**0**	**0**	**2**	**1**	**5**
Convicted persons	**4**	**0**	**0**	**3**	**1**	**8**
Drug trafficking						
Cases associated with the offence	**0**	**0**	**1**	**8**	**15**	**24**
Prosecuted persons	**0**	**0**	**2**	**18**	**34**	**54**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Corruption						
Cases associated with the offence	**0**	**1**	**3**	**13**	**6**	**22**
Prosecuted persons	**0**	**1**	**6**	**34**	**8**	**49**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Tax evasion						
Cases associated with the offence	**0**	**1**	**0**	**0**	**0**	**1**
Prosecuted persons	**0**	**6**	**0**	**0**	**0**	**6**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Organised crime						
Cases associated with the offence	**0**	**0**	**0**	**5**	**8**	**13**
Prosecuted persons	**0**	**0**	**0**	**13**	**17**	**30**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**
Other						
Cases associated with the offence	**1**	**0**	**1**	**4**	**1**	**7**
Prosecuted persons	**1**	**0**	**1**	**4**	**1**	**7**
Convictions	**0**	**0**	**0**	**0**	**0**	**0**

448. Between 2020 and 2024, Armenian authorities initiated 226 ML investigations, which resulted in 80 prosecutions, representing an approximate prosecution rate of 35%. In some complex case examples, the prosecutorial oversight contributed to the inclusion of ML charges alongside the predicate offences. A slight increase in the number of ML prosecutions was noted in 2023 and 2024, particularly in connection with drug-related offences and corruption. Nevertheless, the overall number of ML

prosecutions remains low when compared with the level of underlying predicate criminality[86]. The authorities explained that only part of the predicate crime investigations involve particularly large amounts of proceeds that would potentially lead to a decision to initiate a ML investigation. While this is noted, the resulting ratio of ML prosecutions remains low. For example, of the 931 tax evasion investigations involving "particularly large amounts", only one resulted in an associated ML prosecution.

449. The number of convictions remains low. The previous MER presented data on 13 final convictions and 2 acquittals, whereas during this reporting period the number have decreased - only 7 final convictions, including 3 acquittals. The absence of any sentence imposed during 2021-2022 is considered by the authorities to result from the pandemic's impact on the overall processes in the country. Authorities also indicated that many cases are still pending in the courts due to structural and legislative changes affecting the responsibilities of the courts[87], resulting in delays. It was also noted that the courts face significant resource constraints and an increasing workload, particularly in complex financial cases. The MoJ has requested additional state resources for the judiciary, with limited results. The achieved convictions are not in line with the ML risk profile of the country, as they have been obtained exclusively in small-scale self-laundering cases associated with fraud.

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

450. The sanction for ML offence committed by a natural person is imprisonment. Depending on the severity of the offence, the custodial sentence ranges from a minimum of two years to a maximum of twelve years. Since January 2023, a broad range of criminal sanctions applies to legal persons for any offence, including ML, ranging from fines of up to 20% of the legal person's gross income to temporary suspension of the right to exercise certain type of activity and compulsory liquidation. However, their application is subject to exemptions in certain circumstances (see R.3, c.3.10).

451. During the reporting period, eight custodial sentences were imposed on natural persons, seven of which are final. In all cases, the sentence was imposed for ML in conjunction with the predicate offence.

Table 7.8: Range of custodial sentences imposed for ML (natural persons)

Custodial sentences imposed	2020	2021	2022	2023	2024	Total
Number of custodial sentences imposed	4	0	0	3	1	8[88]
Highest custodial sentence imposed (in months)	30	N/A	N/A	96	84	-
Lowest custodial sentence imposed (in months)	24	N/A	N/A	29	84	-
Average length of custodial sentences (in months)	27	N/A	N/A	52	84	-
Number of suspended custodial sentences	1	N/A	N/A	2	0	3

452. There appears to be an increasing trend in the average length of custodial sentences over the

[86] For example, ML prosecutions associated to drug trafficking account for approx. 0,3% of the total number of drug-related investigations (~8639); the ML prosecutions associated with corruption represent approx. 0,4% of the total number of corruption-related investigations (~5773), while the ML prosecutions associated with tax crime account for approx. 0,06% of the total number of tax evasion related offences (~1459).

[87] E.g., the newly established Anti-corruption court was initially responsible for handling ML-related cases, but these responsibilities were later reassigned to ordinary courts.

[88] According to the authorities, there are seven final convictions. One custodial sentence is being challenged in the Court of Appeals.

period 2020-2024. However, drawing firm conclusions is difficult, given the absence of convictions in 2021 and 2022 and that the 2024 result is based on a single conviction. It was explained that, for six convictions, the custodial sentences were lower (two years on average) due to the small scale of the ML offences[89]. Other two comparatively larger-scale cases resulted in convictions of seven and eight years, indicating a proportionate approach to sentencing.

453. Nevertheless, overall, the results do not suggest that the sanctions applied against natural persons convicted of ML offences, are effective, proportionate and dissuasive. Forty percent of the sanctions imposed on natural persons are suspended custodial sentences, while no sanctions have been applied to legal persons. The larger-scale and more complex ML cases presented to the AT remain pending with no convictions to date. This is despite the authorities' general perception that ML charges have a deterrent effect when applied alongside predicate offenses[90].

7.4. Use of alternative measures

454. The authorities indicated that no cases were identified where alternative criminal justice measures were applied due to the impossibility of securing a ML conviction for justifiable reasons.

455. Although no alternative criminal measures have been applied, authorities informed about one case in which ML prosecution could not be pursued due to the absence of the accused (an international search is ongoing). As an alternative measure, a settlement agreement was reached with the representative of the respondent within civil confiscation proceedings, resulting in the transfer to state of real estate with an estimated market value of EUR 4.6 million.

[89] Laundered property did not exceed EUR 4000.

[90] The maximum custodial penalty for ML (12 years) exceeds those for other serious financial crimes, such as fraud, embezzlement, or tax evasion.

Chapter 8. Asset Recovery

The relevant Immediate Outcomes considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Assets recovery is included as a LEAs' objective through the Anti-corruption Strategies and the AML/CFT/ PFT Strategy which triggered legislative developments and enhanced the mechanisms for the recovery and management of proceeds and property of illicit origin. GPO was given responsibilities in co-ordinating and implementing the civil confiscation regime, which is a positive step in implementing an effective cooperation framework. The rest of the LEAs are responsible to identify and take the necessary assets recovery actions during the investigation in their own cases. However, the results obtained in terms of seizures, confiscations, are not fully convincing that asset recovery is proactively pursued as a policy objective in all ML and proceeds generating cases.

b) Each intelligence and investigative body are responsible to identify and trace criminal property and prepare sufficient evidence in their cases, with a view to confiscation. However, the results obtained so far are not convincing in that asset identification is systematically pursued in pre-trial investigations. Particular difficulties are noted in tracing crypto assets.

c) The authorities have at their disposal the necessary tools to apply provisional measures on criminal property or property of illicit origin. The lack of complete data on applied seizures, hampers the possibility to assess the effectiveness of the overall provisional measures and whether they are commensurate with the estimated volume of the criminal property. The FMC has the power to suspend transactions or business relationships, which contributes to securing criminal property, but this power is rarely used.

d) The AT had access to partial data on property confiscated and voluntarily compensated for certain predicate offences, namely fraud, corruption and tax evasion. Although the results displayed in case of tax evasion appears to be commendable, they seem to mostly reflect voluntary compensations in less serious tax offences during preliminary investigations, and a positive assessment on the overall confiscation regime cannot be made. The introduction of the NCBC regime has enhanced the country's ability to confiscate illicit assets.

e) The declaration requirements under the new EAEU Customs Code for the import/export of cash for personal use exceeding USD 10,000, as well as BNIs, across the customs border of the EAEU, have been applicable in Armenia since 2018. The declared cash over the threshold and BNIs, as well as the identified false/non declarations are communicated to the FMC on regular basis. The IC investigates the criminal cases of triggered by cash/BNI false declarations or non-declarations which are qualified as "smuggling". Out of those cases handed to the IC during the reporting period, 40 – 50 % were closed investigations, after the owner of the cash was identified, admitted the incriminated act and the funds were given to the state on a voluntary basis. No ML or TF cases were initiated on the basis of cash/BNI declarations, consequently, there have been no confiscations of currency or BNIs related to ML/TF.

Key Recommended Actions (KRA)

a) The country should take stock of the overall asset recovery regime at all stages (identification, tracing, seizing and confiscating) to identify the challenges in achieving results aligned with the estimated volume of criminal proceeds and the country risk profile. Subsequent strategic and policy measures should be taken to enhance the institutional framework, provide sufficient guidelines and adequate resources to LEAs on asset recovery matters.

b) Armenia should put in place a system of management of seized property to preserve its value.

c) The country needs to invest in building expertise and resources for tracing, seizing, and confiscating assets. This includes providing law enforcement agencies with the tools, training, and technical expertise to effectively pursue parallel financial investigations and apply provisional measures.

Other Recommended Actions

a) Armenia should establish an efficient system, including centralised, for collecting and analysing data on seized and confiscated property at all stages of the criminal (or civil) process. This would allow for a better understanding of the effectiveness of asset recovery efforts and ensure that authorities can measure their progress against established targets.

b) The FMC should proactively use its authority to suspend transactions and business relationships, while LEAs should request the applications of these powers more frequently, especially in cases involving high-risk financial activities suspected of money laundering and terrorist financing abuse. This would help prevent illicit funds from being transferred or used before they can be properly investigated and confiscated.

c) Given the increasing use of cryptocurrencies in criminal activity, Armenia should establish clear, up-to-date guidelines and procedures for managing and preserving seized crypto assets. This would ensure that cryptocurrencies are not only properly seized but also securely maintained and preserved, reducing the risk of value loss due to fluctuations in the crypto market.

d) The SRC and IC should adopt a more proactive approach to identify and analyse false or non-declarations of cash and BNIs, including systematically assessing any indicators of proceeds of crime and their potential link to ML/TF. This should include enhanced cooperation between the SRC, IC and the FMC.

Overall conclusion on IO.8

Armenia has made significant strides towards establishing a legal and institutional framework for asset recovery as part of its broader anti-corruption and anti-money laundering efforts. Through successive Anti-Corruption Strategies and dedicated AML/CFT/PFT policies, new laws have been adopted (such as the Law on Civil Forfeiture of Illegal Assets), specialised government bodies have been created, and implementation mechanisms have started to take shape. Confiscation efforts of the authorities are primarily focused on recovering the proceeds of domestic predicate crimes in the jurisdiction. Requests for assistance to foreign authorities through official and informal channels are most often used for identifying and recovering illicit assets originating from domestic corruption cases. There are no examples of successful asset recovery from foreign jurisdiction, although asset seizure has been applied in two cases. On a more positive note, the implementation of the NCBC system is progressing well.

Despite advances, asset recovery responsibilities remain dispersed among different agencies (GPO, LEAs, the FMC, etc.), each acting largely within the jurisdiction of their own investigations. While the GPO is tasked with coordinating civil confiscation, there is no overarching authority or cooperation framework to ensure a unified, efficient, and consistent approach to asset tracing, seizing, and confiscation across different types of cases. A strategic weakness is the lack of comprehensive, reliable, and analysed data on asset recovery outcomes, including the value of assets seized and confiscated, the effectiveness of provisional measures, and recovery rates. This impedes evidence-based assessment of the asset recovery system, identification of gaps, and strategic improvements. There is no seized assets management authority. Measures taken against false/undeclared cash movements and associated crimes, such as smuggling, result in fines and confiscations, but the administrative sanctions imposed are not substantial enough to be considered a real deterrent. Additionally, investigations seldom lead to money laundering or terrorist financing charges, suggesting that risks in this area may not be fully appreciated or addressed.

Armenia is rated as having a low level of effectiveness for IO.8.

8.1. Prioritisation of asset recovery as a policy objective and using effective agency structures and cooperation frameworks

8.1.1. Prioritising asset recovery as a policy objective

456. The main policy frameworks addressing strategic objectives related to asset recovery are the Anti-corruption Strategies (AC) 2019-2022 and 2023-2026, and the AML/CFT/ PFT Strategy 2025-2028.

457. Under the 2019-2022 AC Strategy, several developments were made to strengthen the asset recovery system. These include the adoption of the Law on civil forfeiture of illegal assets (LCFIA) in 2020; the approval of the 2020 implementing Government Decision on the procedure for holding a tender for the management of property transferred to the state during confiscation proceeding; and the establishment of a new department within the GPO dedicated to the confiscation of property of illicit origin.

458. The actions planned based on the AC 2023-2026 Strategy aim to further enhance the mechanisms for the recovery and management of corruption proceeds and property of illicit origin. These include six priority actions, including (i) establishing an integrated platform to facilitate information exchange between intelligence units, investigative and prosecutorial bodies and asset recovery specialists; (ii) introducing further amendments to the legal framework on civil forfeiture; (iii) developing a methodology and guidelines for the confiscation of criminal proceeds; and (iv) improving mutual legal assistance mechanisms to facilitate the confiscation of illegal proceeds. While the proposed activities are important, the overall comprehensiveness of the envisaged measures related to asset

recovery appears to be limited. Although the authorities acknowledge that the investigative bodies are essentially the main authorities responsible for tracing, seizure and preparing sufficient evidence for the confiscation of criminal property, they have not been assigned any role in the implementation of these actions. Furthermore, there appears to be a need for more comprehensive and precise budgeting to ensure that sufficient funds are allocated for the effective implementation the AC Strategy and its Action Plan[91].

459. The 2025-2028 AML/CFT/PFT Strategy includes a priority on efficient execution of confiscation. The Action Plan of the Strategy provides for several implementing actions (Actions 10.1 – 10.6). They include the goal to conduct parallel financial investigation, to identify, seize and confiscate criminal property generated by utilising telecommunications and information technologies or derived from drug related offences, corruption and tax crimes, as well as on increasing resources (staff, knowledge and expertise). However, the AT acknowledges that the actual acts based on these priority actions are under the responsibility of each authority and the result are to be seen later. For example, one of the actions from the previous Strategy (2022-2024) that remains unimplemented concerns the improvement of resources available to LEAs for conducting parallel financial investigations (see IO1).

460. The confiscation of criminal proceeds is considered as a policy objective through the above Strategies and action plans. However, the results obtained in terms of seizures, confiscations, are not fully convincing that asset recovery is proactively pursued as a policy objective. Adequate statistics are not kept or analysed to identify trends or gaps in the asset recovery regime. This creates a challenge not only for assessing the overall performance of the framework in place, but also for defining the actual recovery rate of confiscated assets.

8.1.2. Periodic review of asset recovery regime

461. The country has a mechanism to periodically review the strategic steps of asset recovery on corruption crimes and action plan activity performance is verified semi-annually. The AC Strategy 2023 – 2026 is based on the assessment of the results of the previous one, including sections on improving mechanisms for the recovery and management of corruption proceeds and property of illicit origin. This demonstrates a continuous and coherent strategic approach.

462. The Action plan of the AML/CFT/PFT strategy is monitored by the FMC on a semi-annual basis, and, according to the strategy, some drawbacks of and achievements in implementation have already been identified. The commendable periodic reviews are hampered by the deficiencies in collecting up-to-date statistics on asset recovery, in their assessment and the absence of an authority responsible for the oversight of the asset recovery system besides the civil confiscation.

8.1.3. Effective agency structures and cooperation frameworks

463. GPO has responsibilities in co-ordinating and implementing the civil confiscation regime, which is a positive step in implementing an effective cooperation framework in the country. The GPO has clarified the responsibilities of agencies for asset recovery measures in this regard.

464. The rest of the LEAs are responsible to identify and take the necessary assets recovery actions during the investigation in their own cases. Although obligations and powers are regulated and guidance is provided, there are no asset recovery cooperation frameworks. These fragmented efforts may lead to missed opportunities and impair the results in terms of asset recovery.

[91] Armenia: Fifth round of Anti-corruption monitoring follow-up report, OECD (2025), pages 14-17.

8.2. Identifying and tracing criminal property and property of corresponding value

465. Each intelligence and investigative body are responsible to identify and trace criminal property, as well as for preparing sufficient evidence for confiscation in their own cases. Authorities indicated during the on-site visit that investigators, as part of the parallel financial investigations, take mandatory steps to determine the volume of damages, and the availability of funds to ensure compensation. In general terms the investigative authorities confirmed that conducting parallel financial investigation is mandatory in each case with the main sources of information being FI (with court order) and the FMC.

466. Some case studies presented demonstrate the ability of intelligence agencies and investigative authorities to use financial intelligence to identify and trace criminal proceeds. However, the onsite discussions as well as the results obtained so far are not convincing in that asset identification is systematically pursued in pre-trial investigations. In-depth asset investigations are not conducted on a systemic basis, and the competent authorities tend to focus on predicate offences and on swift closure of the cases which restricts detecting and analysing post-predicate offence financial flows, such as ML.

467. A key source of financial intelligence, including banking and BO information, assisting LEAs in identifying and tracing criminal property and property of criminal value, is the FMC. As this intelligence cannot be used as evidence, the access to banking and BO information requires a court order. The available powers are limited in scope and do not provide sufficiently broad access to all the necessary document and information to support the identification and tracing of criminal property. Moreover, about 10% of the total requests to access banking information for evidentiary purposes are rejected by courts (see IO7).

468. One of the biggest challenges is identifying crypto assets, which are increasingly used in money laundering schemes, an emerging threat according to the LEAs met the on-site. While the authorities have presented examples of successfully tracing virtual assets, the only recent establishment of the virtual assets related regulatory framework significantly limits authorities' capacity for their identification, tracing and seizure.

469. Most of the country's crypto-tracing expertise resides within the MIA, which is an intelligence body, but a significant bottleneck is the limited resources available for financial experts in the crypto-field.

470. The competent LEAs have trained employees for asset recovery measures, mostly in certain specialised departments. The investigative bodies have dedicated experts to assist with the parallel financial investigations - IC has 8 experts in financial forensic examination and ACC has 4. Both the IC and ACC are seeking to strengthen their capacity through the recruitment of additional experts.

8.3. Freezing and/or seizing criminal property and property of corresponding value

8.3.1. Active pursuit of provisional measures resulting from financial investigations

471. Armenian legislation provides overall the necessary tools for detecting and restraining the proceeds of crime, whether from domestic or international criminal activity. As in the case of tracing, all LEAs are responsible for tracing and securing criminal assets in the context of their own investigations.

472. The authorities have been able to provide data on property seized during the pre-trial investigation on ML offences (by the IC and ACC) and corruption-related offences (by the ACC) only.

Table 8.1. Property seized in ML cases (source IC)

Year	Number of ML cases where seizure was applied	Value of property (correspondent value) (EUR)
2020	13	301 150 136
2021	15	60 699
2022	16	1 211 205
2023	35	7 044 035
2024	42	6 900 222
Total	121	316 366 297

Table 8.2. Property seized in ML and corruption cases (source ACC)

Year	Value of property (correspondent value) seized in ML cases (EUR)	Value of property (correspondent value) seized in corruption cases (EUR)
2022	45 952	37 953 424
2023	0	386 235
2024	558 036	4 465 041
Total	603 988	37 953 424

473. While in some years the value of the seizures is commensurate with the risk (2020 for example), the value of seized property has varied significantly during the reporting period (see Tables 8.1. and 8.2. above). The authorities explained that this discrepancy results from the calculation method – the large amount seized is linked to a single large-scale case in which seizure measure were initiated in 2020, while most of the assets were in fact seized during 2021-2024. The lack of complete data on applied seizures, hampers the possibility to assess the effectiveness of the overall provisional measures and whether they are commensurate with the estimated volume of the criminal property[92].

Table 8.3. Provisional measures under NCBC (source GPO)

	2021	2022	2023	2024	2025 Sept	Total
Value of total assets seized based on claims (EUR)	14 172 492	171 027 811	841 967 258	219 493 328	80 264 974	1 326 925 863

474. The exact value of seized assets under the civil confiscation regime was not provided, as according to the authorities, statistics are not maintained on the value of property seized. This was explained as in many cases, information on the market value of the restrained property is not available, and in certain instances, the court may lift or modify the applied provisional measure. Nevertheless, according to the authorities, the total included in the last column of Table 8.3. (the overall total for the period) may be considered as approximate amount of seized assets, since provisional measures have been applied in all cases.

475. The FMC has the power to suspend transactions or business relationships, which can also support tracing (as mentioned above), securing criminal property. During the period under review, the FMC

[92] For example, in 2024 alone, over 6,000 investigations were launched for crimes such as fraud, drug trafficking, and tax evasion—crimes that typically generate illicit proceeds.

used these powers in 14 cases, mostly based on FIs notifications but also on the basis of LEA request (1 case). This resulted in the seizure of criminal property worth approximately 2.14 million EUR (see table 8.4. below). While this power could substantially assist in securing funds for further seizure and confiscation (especially when applied at LEA request), it is rarely used in practice.

Table 8.4. Property seized as a result of the FMC's suspension powers (AMD)

	Number of suspension cases*	Value of suspended property (in EUR)	Number of notifications to LEAs	Cases where transactions were unsuspended and notifications where not provided to LEAs	Amount of seized property (in EUR)
2020	1	1,848,772	1		1,815,925
2021	0	-	-	-	-
2022	9	9,925,675	8		619,743
2023	2	1,000,128	1	1	147,236
2024	2	301,425	2		74,463

8.3.2. Expeditious measures

476. To secure possible confiscation, compensation for damages or procedural costs, investigators can adopt a decision on the attachment (arrest) of property, which must be presented for verification to the court within three days[93]. While the process for freezing and seizing property during pre-trial investigations is timely and straightforward, investigative bodies noted that beyond the three days delay, the courts may refuse some requests or requiring difficult-to-obtain documents (*e.g.* expert evaluations of property value). Although clear-cut statistics were not available, these procedural burdens limit the authorities' ability to seize criminal property in a timely manner, especially in cases of electronic property, which can be moved quickly.

8.4. Managing frozen or seized property to preserve its value

477. The management of criminally seized property is fragmented among multiple agencies, depending on the nature of the assets. Precious metals and stones, foreign currency and securities[94] are managed by the Treasury, while local currency is deposited into the bank account of the court dealing with the particular criminal proceeding. Objects other than voluminous property and real estate are managed either by the investigative body that decided on the seizure or by a representative of the local self-government body. Voluminous property is left under the management of the owner, the possessor, an adult family member, or a state authority. There is no designated authority, coordinated management framework or clear rules to ensure the effective preservation of the value of seized property.

478. Property seized under the civil confiscation procedure also falls under the competence of various bodies which may act as the "competent authority". This includes state bodies, local self-government bodies, or state organisations. The legal framework on civil confiscation does not specify the responsible authorities, nor the circumstances under which such responsibilities are assigned. Where preservation of asset value is necessary, assets may be transferred to specialised trust managers. However, it was not in practice, as the necessary legal framework is under development.

479. As mentioned above, the regulatory framework on virtual assets has been introduced only recently and no procedures currently exist for the seizure or management of virtual assets. LEAs have sought assistance from foreign counterparts and discussed domestically to address these issues. Given

[93] Chapter 39 of the CPC

[94] Securities with a value exceeding two hundred times the minimum monthly wage

the increasing use of cryptocurrencies in criminal activity affecting the country, as well as the nature and the fluctuations in value of virtual assets, there is a need for clear and comprehensive guidelines for virtual assets' seizure, management and value preservation.

8.5. Confiscating and enforcing confiscation orders

8.5.1. Criminal property and property of corresponding value located domestically

480. There are no available statistics on the value of confiscated criminal property. The authorities provided partial data on the results obtained in certain crimes: fraud, corruption and tax evasion (see Table 8.5. below), which are based on confiscation orders and on voluntary compensation of damage caused by crime[95] during the preliminary investigations in cases where natural persons were released from criminal liability. Although the results displayed in case of tax evasion appears to be commendable, discussions with the authorities indicate that, in most cases, these amounts represent voluntary compensations rather than property confiscated. A positive assessment on the overall confiscation regime cannot be made.

Table 8.5. Value of property confiscated and voluntarily compensated for certain predicate offences (EUR)

	2020	2021	2022	2023	2024	Total
Fraud	*n/a*	*n/a*	242 857	369 296	105 000	717 153
Corruption	*n/a*	*n/a*	2 079 203	3 034 054	2 585 587	7 698 844
Tax evasion	*n/a*	*n/a*	55 204 258	71 784 444	87 555 555	214 544 257

481. On a more positive note, the introduction of the NCBC regime has started to show results and contributed to the improvement in the country's ability to confiscate illicit assets.

482. The Department for the Confiscation of Property of Illicit Origin (hereafter the Department) within the GPO works with prosecutors and investigative bodies, focusing on civil confiscation. The Department has 12 prosecutors, 2 administrative officers, and 5 financial experts. It initiates civil proceedings against property owners who cannot lawfully justify the origin of assets substantially disproportionate to their legal income.

Table 8.6. Value of property confiscated and recovered based on settlement agreements under NCBC (EUR)

Results of NCBC (EUR)	2023	2024	2025 Sept	Total
Total value confiscated NCBC	4.910.707	6.508.897	1.050.268	12.469.872
ML		4.562.549	1.050.268	5.612.817
Fraud	111.600	0	0	111.600
Drug trafficking	0	0	0	0
Corruption	0	0	0	0
Tax evasion	0	0	0	0
Organised crime	0	0	0	0
Other	4.799.107	1.946.348	0	6.745.455
Total value confiscated NCBC – final decisions	0	0	852.200	852.200
Value of recovered property through settlement agreements	4.973.052	6.508.898	198.068	11.680.018
Total value effectively recovered property NCBC	4.973.052	6.508.898	969.982	12.451.932

483. Through case examples the authorities demonstrated that in 2023, criminal property was

[95] Voluntary compensation of damage – compensation of damage caused by a crime made by a natural person who is released from criminal liability in the event of active repentance, provided that the following conditions are met: i) the person has committed a criminal offence for the first time; ii) the offence is of minor or medium gravity; iii) the person admits the offence and cooperates with the authorities; iv) and compensates for the damage caused by the crime (CC, Article 81).

recovered in four cases based on settlement agreements, while 163 civil forfeiture cases were reviewed in 2024. Approximately 150 civil forfeiture cases are currently pending before the Anti-Corruption Court, most of which are related to corruption offenses.

484. Statistics on the exact value of property seized in NCBC proceedings are not maintained, making it difficult to assess the overall effectiveness of civil confiscation efforts. Most of the criminal property was recovered based on the settlement agreements, while only in one case the this was done based on a final court decision (Table 8.6.). The AT was not informed whether there are cases of extended confiscation under the civil confiscation regime. As indicated under R.4, the extended confiscation mechanism is subject to a technical limitation related to the threshold of 50 million AMD (approximately 120,000 USD) required for applying such measure. This may limit the pursuit of extended confiscation in cases involving assets below this threshold.

8.5.2. Criminal property and property of corresponding value located abroad

485. According to the information provided by the GPO, international information exchange has been used to identify illicit assets linked to proceeds of corruption, fraud and ML, resulting in a total of 12 asset recovery-related requests. In two cases, this led to the seizure of assets (approximatively four years ago), including real estate located in the United States in a corruption case (valued at approximately USD 36 mil.), as well as funds and real estate in a tax related case located in Slovak Republik (valued at approximatively EUR 380 000). None of the seized assets have yet been repatriated (see IO2). This information is partial, as the MoJ does not maintain separate statistics on asset recovery-related requests.

486. During the reporting period, the Department made 46 international requests for identifying assets for recovery by using the CARIN network, but none of those resulted in tangible outcome. There were also 45 MLARs send within NCBC framework, but none ended with a positive response.

487. Based on this information, the AT team cannot conclude that criminal property and property of corresponding value located abroad is effectively recovered.

8.6. Returning confiscated property to victims

488. Returning confiscated property to victims constitutes a priority according to the Armenian authorities. In criminal proceedings, the rights of persons who have suffered material (property) damage are restored through filing a property claim and the full or partial satisfaction of that claim by the court. Notably, according to Article 163 of the CPC, when the victim is deprived of the opportunity to defend their property interests — due to dependence on the accused, being incapacitated or of limited capacity, having mental health issues, or for other reasons — the court has the authority, on its own initiative, to resolve the issue of compensating the damage caused by the crime in the final judicial act.

489. Property may also be returned to victims at the conclusion of a criminal investigation in cases where natural or legal persons are released from criminal liability and voluntary compensate for the damage caused by the crime (CC, Articles 81 and 125). Such measures have been applied in cases involving voluntary compensation by natural persons. As shown in Table 8.7, there is no breakdown by the means through which property was returned to victims. However, based on the discussions with authorities, it appears that the return of property through voluntary compensation of damages occurs frequently. There is no data on the total value of property claims, which prevents the assessment of the extent to which property is returned to victims.

Table 8.7. Value of property returned to victims based on confiscation orders and voluntary compensation of damages (EUR)

Year	Natural persons	Legal persons
2020	1,023,038	128,424
2021	739,184	232,947
2022	344,624	723,790
2023	1,373,737	772,304
2024	2,786,366	473,648

8.7. Identifying and confiscating falsely or undeclared currency/BNIs or those related to ML/TF or predicate offences

8.7.1. Identifying and seizing non-declared or falsely declared cross border movements of currency and BNI

490. Armenia shares borders with Georgia, Iran, Turkey, and Azerbaijan. Only the borders with Georgia and Iran are open, and there is one international airport operating from Yerevan. The smuggling department of the SRC has customs officials at all open border points, working with border control units to identify undeclared cash and bearer negotiable instruments (BNIs). X-ray technology and personal searches are used when necessary.

491. Armenia introduced a written declaration system in 2007, while new declaration requirements for the import and export of cash and BNIs across EAEU borders have been applicable under the new EAEU Customs Code since 2018. Cash declarations exceeding the USD 10,000 threshold, all declared BNIs, as well as the identified false/non declarations are communicated to the FMC on regular basis.

Table 8.8. Cross border declarations and enforcement actions (EUR)

Year	Declarations	Value	Non-declarations	False declarations	Administrative enforcement actions	Fines imposed (value)	Investigations[96]	Prosecutions	Cash seized[97]	Cash confiscated	Voluntary compensation of damage
2020	310	25,907,307	0	0	0	0	0	0	-	0	0
2021	42	2,479,727	7	0	3	350	4	3	-	0	48,896
2022	1,310	74,812,102	3	0	1	116	3	0	-	0	2, 222
2023	2,117	125,774,811	7	0	9	9483	7	0	-	158,053	986,040
2024	970	51,398,523	23	0	37	29348	21	7	-	45,444	41,120

492. According to the data provided (Table 8.8.), there are no cases of false declarations, while the number of non-declarations of cross-border cash remains relatively low, with a slight increase observed in 2024. Nonetheless, during the on-site, authorities gave a case example, investigated by the IC, of

[96] All investigations were initiated for cash smuggling.

[97] Please note that there is no seizure applied in these cases, however the assets are secured as evidence.

drugs smuggled from Iran to Armenia in an organised matter. The funds flow from Armenia to Iran was carried out through land border, by money mules transporting cash piles amounting USD 7 000 on each border crossing. The method, which was used to smuggle a total of 10 million USDs, was implemented to avoid the cash control and declaration system and potential seizure of the proceeds. Although Armenia is not regarded as a transit country for drug smuggling (according to the NRA), the above case example appears to indicate the opposite. The AT is not aware of any restrictive measures applied by the SRC in this particular case.

8.7.2. Confiscation of currency or BNI related to ML/TF or predicate offences

493. The country has no technical obstacles to confiscate cash and BNI in criminal proceedings. As the Table 8.8. shows, during the period under review, there has been confiscations based on non-declaration of cash totalling 203 497 EUR.

494. The IC investigates most criminal cases triggered by cash/BNI false declarations or non-declarations which are qualified as *"smuggling"*. Out of those cases, during the reporting period, 40 – 50 % are closed investigations, after the owner of the cash was identified, admitted the incriminated act and the funds were voluntarily given to the state. In such a way the authorities were able to recover an additional 1 078 278 EUR.

495. No ML or TF cases were initiated on the basis of cash/BNI declarations. The authorities claim that the possibility of ML is considered and investigated, including through parallel financial analysis and that no ML/FT suspicions has been identified. Nevertheless, based on typologies presented, as well as some of the NRA conclusions, it is difficult to concur that there is no risk of funds generated by predicate offences transiting the border in the form of cash.

8.7.3. Sanctions

496. When undeclared cash/BNI is found, the SRC launches administrative proceedings (Law on Customs Regulation). During the period under review, 50 such proceedings were initiated, with an overall value of the fine imposed of 39 297 EURO. The value of the administrative sanctions cannot be considered neither effective, proportionate or dissuasive (see R.32).

497. If the amount of undeclared cash/BNI exceeds 20 000 USD, the case is subject to criminal proceedings and handed immediately to the IC. Information on the number of convictions and criminal sanctions imposed in the cash smuggling related cases was not made available to the AT.

Chapter 9. Terrorist Financing Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Armenia has systems in place to identify, investigate and prosecute TF, and the relevant authorities are adequately trained and resourced. The authorities look for possible TF activity in all cases of suspected terrorism or from TF-related STRs. However, the use of funds raised through other forms of criminality for TF purposes and possible TF involvement in transactions linked to high-risk countries are not sufficiently explored. The ability to identify TF is also limited by underreporting of suspected TF by the private sector, with only 5 TF related STRS received during the assessment period, which has a cascading effect.

b) A wide range of investigative powers is available to the authorities in TF cases. During the assessment period there was one TF investigation, and some aspects of this are ongoing.

c) There have been no TF prosecutions or convictions to date and therefore no sanctions for TF have been applied. However, in most respects the necessary sanctions are available under the legal framework and the prosecutors, and the courts have the necessary resources to deal with TF cases.

d) TF is integrated into counter terrorism strategies but overall, there is scope for a greater focus on TF at a national level. The authorities generally collaborate well on counter terrorism issues, but there is scope for greater sharing of information and intelligence to support counter-terrorism efforts.

e) Armenia has measures in place that could be used as alternatives to TF convictions, but (except for making a designation under UNSCR 1373) they have not been used in practice.

Key Recommended Actions (KRA)

a) The authorities should be provided with training and guidance on identifying possible TF and terrorist assets from cases involving criminality other than terrorism.

b) Guidance or other outreach focused on TF should be provided to reporting entities to enable them to identify and report possible TF activity.

c) The NSS and the IC should put in place procedures or other measures to ensure that possible TF involvement in transactions to high-risk countries are routinely explored.

Other Recommended Actions

a) Armenia should implement national strategies and activities that are more targeted at TF activity and terrorist assets.

b) Armenia should implement Memoranda of Understanding or similar measures to promote greater sharing and use of information and intelligence between all authorities on matters that may involve possible TF activity.

Overall conclusion on IO.9

Armenia has the necessary institutional framework for the identification, investigation and prosecution of TF and the authorities appear adequately structured, trained and resourced in this area. Appropriate steps are taken to identify possible TF activity from terrorism investigations and STRs related to TF. There has been one TF investigation during the assessment period, some aspects of which are ongoing, and information from this investigation was used to support designations under UNSCR 1373. There have been no TF prosecutions or convictions to date, but there are no legal or procedural obstacles to prevent this or the imposition of appropriate sanctions in most cases. TF is integrated into counter terrorism strategies to some extent, and the authorities generally collaborate well on counter terrorism issues at both a strategic and operational level. There are alternative measures to TF convictions available to the authorities, although these have not been used in practice.

However, while the outcomes achieved are broadly in line with Armenia's understanding of its TF risk profile (see also IO.1), there is reason to believe that the authorities have not always taken steps to identify cases where funds raised through predicate criminality are used for TF purposes, or fully to use information or intelligence that might disclose TF. There is also evidence of underreporting on TF by the private sector. These are significant concerns, given the impact that shortcomings in identification of TF activity inevitably have on the jurisdiction's ability to investigate and prosecute TF offences. Furthermore, there is scope for a greater focus on TF in strategies and activities at national level.

Armenia is rated as having a moderate level of effectiveness for IO.9.

9.1. TF activity identified and investigated

9.1.1. Identification and investigation of TF activity

498. Armenia has the necessary systems in place for the identification and investigation of TF, with clear delineation of responsibilities. The relevant authorities are the FMC and the NSS at an intelligence level, and the IC at the investigatory level. At the beginning of the assessment period, both the NSS and the IC were responsible for investigating TF, but following a government decree in 2024, the investigative arm of the NSS was absorbed into the IC, which now has sole responsibility for TF investigations. According to the authorities this did not lead to any noticeable loss of expertise, as most of the investigators from the NSS transferred into the IC.

499. The authorities appear to be structured, trained and resourced to an appropriate level to discharge their functions. The FMC has two analysts who are TF specialists, and other analysts also receive regular TF training so are able to deal with TF cases. Under the FMC's STR Prioritisation Rules, all TF related STRs are treated as a very high priority, which is the top priority rating. For reasons of national security, the NSS did not provide information about how it is structured, trained and resourced, but stated that it had no concerns on these fronts. The authorities also confirmed that these issues are routinely reviewed and fine-tuned as required The IC's central department is responsible for specialist

matters such as TF. It has a total number of 39 investigators, including 5 who are specialists in terrorism and TF, although other investigators are also able to take on TF cases. All investigators take part in regular TF training, including under programmes organised by the Academy of Justice.

500. By way of example, the authorities in cooperation with the Council of Europe organised a workshop on Investigation and Prosecution of Terrorist Financing Cases in October 2023 attended by investigators, the FMC prosecutors and judges on, among other things, current/emerging terrorist financing threats and vulnerabilities; effective institutional structures, organisational roles and responsibilities among national institutions for countering TF; the importance of joint investigative teams; the terrorist financing cycle (including the differences between ML and TF); how terrorist groups raise and move funds; the best practices in investigating and prosecuting TF; and TF typologies.

Identification of TF activity

501. Possible TF activity may be identified from investigations into suspected terrorism or other criminality. TF investigations may also be initiated by the IC on the basis of financial intelligence via referrals from the NSS. The referral process includes FMC input, as the FMC disseminates TF related intelligence from STRs or other sources (e.g. alerts from international partners) to the NSS. The NSS develops this intelligence and then considers whether to refer the case to the IC for investigation. The NSS and the IC may continue to liaise with the FMC as required during the progression of any matter.

502. Five TF related STRs were received by the FMC from the private sector in the assessment period, primarily arising from suspected matches with persons who had been identified in other jurisdictions as having terrorism links. The FMC carried out analysis and made disseminations to the NSS, which then made additional enquiries. However, no TF activity was identified in any of these cases.

Box 9.1. Case Studies – STRs relating to possible TF

Case 1

In 2021 a bank submitted an STR stating that Non-Resident Natural Person 1, accompanied by another individual, approached a branch of the bank and asked to open accounts on an urgent basis, explaining the haste by the need to leave the country on the same day. When asked about the purpose of opening the accounts, Non-Resident Natural Person 1 provided unreliable explanations. She further informed the Bank that her husband, Non-Resident Natural Person 2, would arrive in Armenia within a month.

Adverse information was identified through Internet searches and the World-Check database, indicating that both Natural Person 1 and Natural Person 2 had been arrested in Turkey in 2017 on suspicion of involvement in terrorist activities.

The bank rejected the request to open bank accounts for Natural Person 1. Although no financial transactions were conducted by the individuals, due to the adverse information suggesting possible links to terrorism, the STR was classified as “Very High Priority.” The entire analysis — including detailed CDD information (e.g. phone number, address, Facebook profile, and copies of adverse media reports) — was disseminated to the NSS for appropriate action. Following activity by the NSS, no criminality was identified.

Case 2

In 2023, a Non-Resident Natural Person approached a bank to obtain a personal bank card in Armenian drams and open a USD account for an entity registered in Armenia under his name. To substantiate his income, the individual presented a service contract between the entity and a foreign company under which specified payments would be made. However, the contract was dated after the attempted opening of the account and would not be finalised until after activation of the account. The bank declined to provide the bank card or to open the account, and submitted an STR.

The FMC carried out analysis using information from both restricted-access databases and public information. This established that the individual had recently acquired the right to reside in Armenian and had been designated on the Russian FIU's terrorist and extremist list following a conviction for participation in terrorist acts in Russia for which he had served a prison sentence. No further financial activity was identified in FMC databases or the Central Registry of Accounts.

Findings of the analysis were disseminated to relevant Armenian law enforcement authorities, as well as to the Russian FIU. According to the feedback received following preventive measures carried out by law enforcement authorities, no high-risk indicators or issues of concern were identified. Given the individual's terrorist designation in Russia and the suspicious timing and nature of his attempted engagement with Armenian banks, it was assessed that the primary motive was likely to be to circumvent restrictions on the Russian financial system.

Source: FMC

509. To date the NSS has made no TF referrals to the IC, although it has made some referrals for terrorism cases. These referrals have resulted in 13 terrorism investigations, all of which have been overseen by specialist prosecutors. None involved legal persons. According to the IC and as confirmed by the GPO, TF has also been considered in each of these investigations. Financial flows of suspects, their relatives and associates have been looked at, with the assistance of the FMC. Applications have also made to the court to obtain access to banking information, and at the time of the onsite visit there were 6 such cases before the court. However, apart from the ongoing aspects of the TF investigation referred to below, all of the terrorism cases that have been investigated during the assessment period have involved self-funding, so no TF investigations were initiated.

Box 9.2. Case Study – Financial Enquiries in a Terrorism Investigation

Person A was under investigation for organizing a terrorist act with the intention of intimidating a political party and forcing the public authorities to carry out or refrain from certain actions. This involved arranging explosions near a petrol station and at a private residence. Person A also liaised with three associates who assisted with planting the explosive devices.

Throughout the course of the investigation, financing aspects were also examined. In particular, the following actions were taken:

- Banking information relating to all of the persons involved in the case was obtained;
- Operational-intelligence bodies looked into the financial and property status of these persons and their sources of income;
- The financial and property capabilities of persons associated with these persons were also checked, including through inquiries made to a number of state bodies.

These enquiries established that the activities of Person A were self-funded and did not reveal any indications of financing by any other source.

See also the case study about a terrorism investigation under IO10.

Source: GPO

510. The AT was satisfied that where there are TF related STRs or terrorism investigations, the authorities take appropriate action to identify possible TF activity. The AT therefore has no reason to question the outcomes in these cases, which are in line with Armenia's understanding of its risk profile for TF (although see issues around the assessment of TF risk identified under IO.1).

511. However, the very low number of TF related STRs calls into question the level of TF understanding and reporting by the private sector. This has a cascading effect that undermines the ability of the authorities to identify possible TF cases. The AT also has concerns about the identification of

possible TF activity from other sources. According to the IC, TF is routinely considered in investigations into other offences such as drug trafficking that are recognised internationally as being linked to TF. An example was given of a large-scale drugs case.

Box 9.3. Case Study – Actions Taken to Explore Potential TF in Drug Smuggling Case

The police from the Ministry of Internal Affairs found that a group of individuals was involved in smuggling drugs into Armenia for sale within the country. It was found from phone communications that the profits were regularly cashed out and transferred to Person A. The Police referred the case to the IC, which opened a case on drug smuggling.

Since some of the intercepted messages included vague phrases, and some of the transfers were made to people who did not appear to have any clear connection to the group; the IC decided to also examine whether there were any possible TF elements in the case, as part of a parallel financial investigation. Specifically, during the course of the investigation the following measures were taken in respect of Person A, the group and persons associated with the group:

- Their financial transactions including cash movements, were analyzed
- Their details (including all possible publicly available data) were cross-checked with specific TF-related databases and lists established in accordance with United Nations Security Council Resolutions.
- Their possible links or association with any non-profit organizations were examined.
- Their travel patterns were explored and when applicable were mapped, including with border crossing information.

Ultimately, the probe into potential TF revealed that the communications were non-ideological, and that the transfers were basically settlements for internal debts within the network that the group participated in.

The investigation, at the same time, established that:

- There were no signals or any other type of indication of TF; whereby none of the funds were collected, provided, or intended for use for TF purposes of in support of terrorist groups.
- None of the beneficiaries, the members of the group or persons associated with the had links with jurisdictions that were high-risk for TF.
- No operational evidence supported the existence of a TF network behind the scheme.

Consequently, the IC did not further consider the TF aspect of the case, while the main criminal proceeding continued in relation to drug smuggling.

512. The AT was satisfied that in this case; appropriate steps were taken to look for possible TF. However, no other examples were provided of any case where possible TF was considered in relation to predicate criminality. Therefore, the extent to which Armenia is proactively looking to identify possible TF activity in non-terrorism investigations was not demonstrated.

513. Concerns about non-identification of TF also arise from an example provided to the AT of an intelligence report from the FMC to the NSS. This report was based on intelligence received by the FMC under the “Regional level operation” programme, through which FIUs in the CIS countries share data on cross -border money flows for strategic purposes. Further information provided by the authorities demonstrated that the intelligence concerned a total of 261 transfers to 5 jurisdictions that are high-risk from a terrorism /TF perspective from money services providers within Armenian banks. Preliminary analysis by the FMC on some of these transfers indicated that there was no obvious rationale for them. The proactive and collaborative approach taken by the FMC on receiving this information is commendable. However, none of the Armenian banks in question had made any STRs

about these transfers.

514. The authorities clarified that in the case of one of the jurisdictions in question, three transfers to the same recipient were made from three separate Armenian banks, and as none of the individual banks were aware of the other transfers this would not necessarily have been seen as suspicious. The authorities also clarified that the NSS had looked into these transfers and confirmed that they appeared to be for legitimate business reasons.

515. While these further explanations are useful in allaying concerns about these particular transfers, they do not explain the lack of any STRs in relation to the remaining 258 transfers to high-risk jurisdictions. This therefore further calls into question the level of TF understanding and reporting by the private sector, which suggests that the list of jurisdictions that are high risk for TF which is regularly updated and communicated to reporting entities is not being fully utilised to identify possible TF links to the movement of funds involving those jurisdictions. Furthermore, no information was provided by Armenia about any action taken by the NSS in relation to any of those 258 transfers in response to the report from the FMC. This suggests that TF intelligence reports other than STRs are not fully used to identify TF activity.

Investigation of TF

516. During the assessment period there was one TF investigation, which was carried out by the NSS. Although the case resulted in a conviction for terrorism related offences, no TF prosecution was brought because the evidence indicated that the suspects were self -funding. However, some other aspects of the TF investigation are ongoing, but for reasons of operational security no further details could be provided.

517. The FMC and the GPO have jointly produced a document entitled Technical Guidance on Investigation into TF Offences which has been endorsed by the Interagency Committee. However, this document was only recently issued so had not yet been applied in practice at the time of the onsite visit.

518. The IC confirmed that it has a wide range of investigatory powers available to it, including the use of special investigative techniques, and all necessary measures are in place to enable the sharing of sensitive material of the kind that is likely to arise in TF cases. However, the limitations on powers to use compulsory measures for the production of records held by FIs, DNFBPs and other natural or legal persons identified under Recommendation 31 and further elaborated under Immediate Outcome 7 are also relevant to TF investigations, as are the potential restrictions on the capacity to investigate legal persons identified under Immediate Outcome 7.

9.1.2. Investigations identifying the specific role of terrorist financier

519. As explained above, there has only been one TF investigation in the assessment period, which cannot be further described as some aspects are ongoing. Therefore, it is not possible to determine the extent to which the investigation has identified the specific role of terrorist financiers. However, taking into account the steps taken by the authorities to look for financial flows with third parties in terrorism investigations, the AT has no reason to doubt that this would be considered as part of a TF investigation.

9.2. Prosecuting and convicting different types of TF

520. In the absence of any concluded TF investigation to date, there have been no prosecutions or convictions for TF. However, there have been 8 terrorism prosecutions, which were taken forward by specialist prosecutors within the GPO. The prosecutors confirmed that in all of these cases possible TF had been considered. The AT was satisfied the GPO has the necessary expertise and training to conduct a TF prosecution if that should arise (and note that prosecutors also took part in the training event in October 2023 on TF investigation and prosecution described above).

521. There are no specialist judges for terrorism and TF cases, but all judges receive training on these topics (and as indicated above, the judiciary participated in the training event in October 2023). Armenia has no special courts or court procedures for dealing specifically with terrorism or TF, but the judiciary confirmed that there are procedures in place to enable closed hearings in cases involving matters of national security and the 8 terrorism prosecutions were dealt with in courts of general jurisdiction. The judiciary also confirmed that they did not believe there to be any legal obstacles to bringing a successful TF prosecution. The AT therefore has no reason to doubt that Armenia has the capacity to take forward TF prosecutions and achieve convictions (subject however to the limitations on court resources noted under Immediate Outcome 7).

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

522. As there have been no TF convictions to date, no sanctions have been applied for this offence. However, the necessary sanctions are available to the courts, subject to some restrictions on the sanctions applicable to legal persons (see Recommendation 5). Although sanctions have been imposed in some terrorism cases, no details were provided so it was not possible to assess from this the way that the courts would be likely to treat terrorism related activity.

9.4. National counter-terrorism strategies and activities

9.4.1. Formulating national counter-terrorism strategies and activities

523. Armenia has enacted AML/CTF/CPF National Strategies for 2022-2024 and for 2025 - 2028, both of which are supported by action plans (see under PF). It also has a Strategy for Combatting Terrorism, although this was not available to the AT. There have been no TF prosecutions or convictions that could inform any of these strategies, but there have been TF investigations which could be used for this purpose.

524. The AML/CTF/CPF National Strategy for 2022-2024 specifically envisaged the integration of TF investigations into the Action Plan deriving from the Strategy for Combatting Terrorism. However, no information was provided about any measures that were implemented to achieve this in practice.

525. The 2025 – 2028 AML/CTF/CPF National Strategy and action plan contain some measures that are specifically aimed at TF, namely the use of information on counter terrorism and related assets to support designations for TFS, conducting parallel financial in terrorism alerts or cases to identify TF, and incorporating technical guidance in the training programs for law enforcement bodies.

526. Nevertheless, as explained under Immediate Outcome 1 the overall focus on TF in both of the AML/CFT/CFP strategies is limited. TF is primarily referenced in conjunction with ML and there is little or no consideration of the ways in the strategic approach to TF should be different from that for ML or on ways to address specific TF threats or vulnerabilities disclosed by TF investigations. In addition, some key aspects are entirely focused on ML without reference to TF at all (e.g. the provisions in the 2025- 2028 strategy dealing with confiscation, which only address the proceeds of ML and predicate criminality and make no reference to terrorist assets). Furthermore, neither the 2022-2024 strategy nor the 2025- 2028 strategy addresses the use of information from non-terrorism cases to identify possible TF activity or terrorist assets. In the view of the AT, while the disparity in focus between ML and TF is in line with Armenia's risk profile to some extent and the existing strategies and action plans provide a foundation for addressing TF at a national level, more needs to be done to develop a targeted approach in this area.

9.4.2. Sharing and using information and intelligence to support national counter-terrorism purposes and activities

527. Overall, the authorities demonstrated the effective sharing and use of information and intelligence in relation to terrorism investigations and prosecutions.

Box 9.4. Case Study – Sharing and using information and intelligence in a terrorism case

In 2023, the NSS initiated an investigation under the supervision of the GPO concerning 5 Armenian citizens suspected of organizing and preparing acts of terrorism within Armenia. The investigation established that the suspects were engaged in the illegal acquisition, transportation, storage, and carrying of firearms and ammunition, with the intention to use them for acts aimed at intimidation and an attack against a public building. The group also carried out recruitment activity in order to increase operational capability, procured or adapted equipment including firearms and munitions, military-style clothing and accessories and communications apparatus, and developed methods to weaponize commercially-produced unmanned aerial vehicles. The NSS carried out operational-search measures to prevent the potential terrorist act and to identify all of the individuals, which included the use of surveillance and interception of communications.

The hypothesis of possible financing by third parties to the individuals, both from within Armenia and abroad, was also explored. However, this did not reveal any credible or likely indications of TF, as the individuals only utilized their own financial means.

The NSS cooperated closely with the Investigative Committee and the GPO. These prompt and coordinated actions successfully prevented the realization of a potential terrorist act, and the collected evidence, including seized weapons and communications data, was transferred to the Investigative Committee for further procedural action. The coordination between security and judicial authorities enabled the full application of counter-terrorism procedures to ensure that no elements of organized terrorism, terrorist financing, or cross-border linkages existed.

Source: NSS

528. In addition to the sharing and use of information and intelligence for the purposes of terrorism investigations, information obtained in the course of the 2020 TF investigation was used to support designations under UNSCR 1373 (see IO10). There was also effective collaboration between the GPO and the FMC in relation to the development of the Technical Guidance on Investigation into TF Offences referred to under Core Issue 9.1, which was carried out to address Strategic Task 1.18 in the need identified in the AML/CTF/CPF National Strategy for 2022-2024.

529. However, the failure to follow up on suspicious money flows to jurisdictions that are high risk for terrorism and TF and the fact that only one example was provided where TF links to predicate criminality were explored indicate that there is nonetheless scope for greater sharing and use of information and intelligence to support national counter-terrorism efforts.

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

530. To date, no alternative measures have been used where a TF conviction is not possible. However, there is a range of such measures available to the authorities that could be used for this purpose. These include the withdrawal of passports or nationality, denying entry into the country, extradition and deportation. Furthermore, as explained under IO10, Armenia has made designations under UNSCR 1373.

Chapter 10. Terrorist Financing Preventive Measures and Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Armenia implements TFS for TF without delay. Designations under UNSCRs 1267/1989/2253 and 1373 become immediately effective in domestic law. While all policies and procedures are in place for making designations under UNSCR 1373, there is no guidance to assist other jurisdictions in making designation requests. The FMC promptly communicates updates- primarily to banks-while other reporting entities rely on voluntary subscription or independent monitoring of UN lists via the FMC website.

b) No assets or funds have been frozen under TF-related UNSCRs, which is broadly consistent with Armenia's view of its risk profile. Domestic designations under UNSCR 1373 were made swiftly and in line with procedures, though no assets were identified in practice.

c) Armenia has identified the subset of NPOs falling under FATF definition and assessed their TF risk as low. While outreach has been conducted, NPOs met onsite demonstrated limited awareness of how NPOs may be misused for TF. Nevertheless, they all had robust financial controls in place.

d) Mitigating measures are applicable to all NPOs so are not risk based. For most of the assessment period there was no oversight of compliance with these measures, and although Armenia has established a framework for targeted oversight of higher-risk NPOs and initiated preliminary engagement, this framework was only introduced towards the end of assessment period and has not yet been implemented, preventing full assessment of its effectiveness.

e) Banks and larger non-banking FIs demonstrate good understanding of their TFS obligations and have effective screening mechanisms in place. Smaller FIs and DNFBPs rely on manual checks but given their simple, domestic client base, their risk exposure is limited.

f) Thematic inspections of banks indicate that screening systems operate effectively, with only operational deficiencies identified. Understanding of sanctions evasion is well developed among banks and FIs with cross-border exposure but remains less mature among smaller FIs and DNFBPs, in line with their business model and risk exposure.

g) Competent authorities have strengthened TFS awareness through sustained outreach and training, and reporting entities generally demonstrate good understanding of their obligations.

h) Supervisory engagement with banks is robust and includes regular testing of their TFS controls, while supervision of non-banks FIs and DNFBPs is more limited. Supervision generally focuses mainly on screening obligations and broader sanctions-evasions risks are covered to a more limited extent.

Key Recommended Actions (KRA)

No KRAs.

Other Recommended Actions

a) Armenian supervisory authorities should develop further guidance on TF sanctions evasion typologies and ensure smaller FIs and DNFBPs receive tailored outreach that reflects their specific business models and risk exposure. The supervisory engagement with non-bank FIs and DNFBPs should be enhanced and expand its focus beyond screening processes to include sanctions evasions risks and practical vulnerabilities.

b) Armenia should consider developing clear guidance for foreign authorities on submitting designations requests, including required information, communication channels and contact points.

c) The authorities should take further steps to implement a risk-based approach to the oversight of the NPO sector; this should include a review of the obligations applicable to NPOs and the framework for oversight and enforcement of those obligations to ensure that measures applicable to NPOs are risk based and can be enforced.

d) The authorities should carry out additional outreach to NPOs, particularly those assessed as higher risk, to improve their understanding of TF typologies and misuse scenarios.

Overall conclusion on IO.10

TFS related to TF are implemented without delay. Armenia has made designations under UNSCR 1373 but has not made a designation proposal to the UN or another jurisdiction and has not received a designation from another jurisdiction. No assets linked to designated persons have been identified, but instrumentalities of terrorism have been recovered by the authorities. While the limitations on identifying TF identified under IO9 may have some effect on the ability to identify terrorist assets, these outcomes are broadly in line with Armenia's risks. While Armenia has assessed the TF risks of the NPO sector, the requirements applicable to the sector are not risk based. For most of the assessment period the sector has not been subject to any oversight of compliance with those requirements, and although some steps have been recently taken to initiate risk-based oversight of NPOs, this has not yet been implemented. Furthermore, the understanding of TF risks by some NPOs is limited. However, the materiality of these various deficiencies in relation to NPOs is limited, given the risk profile of the sector, and the controls that NPOs have in place.

Understanding and compliance of reporting entities as regards TFS obligations is good, subject to some deficiencies which are not material from a risk perspective. The authorities generally take appropriate measures to monitor and ensure compliance with TFS, but more should be done in relation to sanctions evasion. However, the materiality of this is limited, as the only sectors likely to be exposed to sanctions evasion in practice have a good understanding about this issue.

Armenia is rated as having a substantial level of effectiveness for IO.10.

10.1. Implementation of TF-related targeted financial sanctions without delay

531. Under the AML/CFT Law, financial institutions and DNFBPs are obliged to freeze the assets of persons designated by the UN under UNSCR 1267 and successor resolutions without delay, and to prohibit the making of funds or economic resources available to them. The same applies designations made by Armenia under UNSCR 1373. Therefore, under Armenian law, designations and any changes to designations under these UNSCRS are immediately effective without the need for any additional measures to be taken by the authorities.

532. The FMC is responsible for communicating changes to designations to the reporting entities. Chapter 26 of the FMC's Operational Manual, supported by an internal Order of the Head of the FMC, sets out the respective process. The International Relations Division of the FMC checks the UN sanctions lists every working day. Any changes are communicated immediately to FMC's Information Systems Design and Development Division, which manually updates the FMC database of designated persons and posts an update on the news section of the FMC website. The FMC also sends electronic notifications of changes to all banks. Other reporting entities will only receive notifications if they subscribe to a mailing list. The authorities were unable to confirm the proportion of reporting entities that have subscribed, as both personal and professional personal email addresses may be used.

533. FMC notifications are usually sent out on the same day that a change occurs, as confirmed by examples provided to the AT. In addition, the FMC has recently issued a formal communication to instruct reporting entities to monitor UN lists independently of FMC notifications. To facilitate this, there is a dedicated page on the FMC website with a searchable interface that enables any person to check names against the UN sanctions lists.

534. There is a procedure in place for making designation recommendations to the UN under UNSCR 1267 and successor resolutions, designations under UNSCR 1373 (whether autonomously or at the request of another jurisdiction), and designation requests to other jurisdictions. This procedure is set out in the Listing Rules (see R.6), which have been in place throughout the assessment period. The FMC has a central role in this procedure, which is formalized and governed by the FMC's Operational Manual. The Listing Rules and the FMC Operational Manual between them extend to all of the activity necessary to make designation proposals, designations and designation requests. However, while the Listing Rules are publicly available and therefore accessible to other jurisdictions who might wish to make a designation request, the AT considers that additional guidance would be beneficial (e.g. by setting out the kind of information other jurisdictions should provide, communication channels and contact points etc.).

535. No request to freeze assets has been made to, or received from, another jurisdiction, so these aspects of the system have not been tested. However, Armenia made domestic designations on two occasions under UNSCR 1373 (December 2020 and October 2021), designating a total of 341 individuals and 13 entities. These designations remain in place. In both cases, the authorities acted quickly to obtain and assess information from a wide range of domestic and international sources. Once this had been done, the designations were made in a matter of days. Therefore, Armenia was able to demonstrate the ability to apply its procedures effectively in practice (as confirmed by redacted minutes of the relevant meeting of the Interagency Committee). In both cases, the designations were communicated to the reporting entities on the same day that they were made. These designations have not resulted in the identification of any relevant assets within Armenia, because according to the authorities, the designated persons have not used Armenia's financial or non-financial systems and have

not carried out any activity within the territory of Armenia.

536. The authorities had considered making designation proposals to the UN for persons designated domestically but concluded that the criteria under relevant UNSCRs were not met. The authorities also explained their reasons for not requesting any other jurisdiction to freeze the assets of the persons whom they had designated. While further details are not provided here on the grounds of sensitivity, the AT is satisfied that the reasons were valid.

537. Reporting entities are required to carry out sanctions screening and to report any matches to the FMC. These obligations are supported by Freezing Guidance issued by the FMC (see R.6), and by the template for making STRs referred to under IO.6 which includes a specific section for reporting sanctions matches. In addition, all STRs received by the FMC are systematically cross checked against UN lists for possible matches. The authorities advised that this independent secondary verification is carried out to ensure that any positive matches which may have been overlooked or misidentified are promptly detected.

538. To date, no assets have been frozen under UNSCR 1267 and successor resolutions. Armenia's designations under UNSCR 1373 have also not resulted in the freezing of any assets.

539. However, Armenia's systems for identifying assets linked to persons designated under other sanctions matches have been tested by examples of suspected matches under other regimes. As explained under IO.11, assets linked to persons designated under PF sanctions regimes have been identified and frozen. There has also been a case where a potential link to a designated person was reported and looked into by the authorities but turned out to be a false positive.

Box 10.1. Case Study – Suspected Sanctions Match

In 2023, Armenian resident Person A, using his own account held with Bank 1, attempted to make a transfer to the account of a foreign resident: Person B in Jurisdiction C. When conducting CDD, the internal system of Bank 1 identified a match with an individual subject to targeted financial sanctions established pursuant to a UNSCR. At that stage, the only information that Bank 1 had on Person B was: the name and last name, the bank details of Person B, and the justification of the attempted transaction, noted as "payment for design services".

Following the match, Bank 1 immediately froze the funds relating to the transfer and contacted the FMC. The FMC instructed Bank 1 to seek further information from Person A about Person B, including requesting copies of any documents available. Person A provided a copy of Person B's passport to Bank 1, which then provided it to the FMC.

The FMC decided to apply additional screening measures for gathering further information, namely by:

- Quickly screening Person B against all available databases;
- Initiating analysis on Person B using social media;
- Quickly screened Person A, namely via the quick access to the designated database of the SRC.

The additional screening measures employed by the FMC revealed the following:

- The date of birth of Person B did not match with the date of birth of the individual subject to TFS established pursuant to a UNSCR.
- Person B's name and last name were very common both in Jurisdiction C, as well as in the wider region; and that Person B was indeed a moderately-known freelancer, who specialized in interior design.
- Person A's business activity was in line with the justification of the transaction, as main area or activity of Sole Proprietor A was "design and construction".

Consequently, it was quickly established that Person B did not have any relation to the individual subject to targeted financial sanctions established pursuant to a UNSCR, and the apparent match was a false positive. The entire process took only one hour. Bank 1 was then instructed to lift the freezing measure and not to file a formal STR.

Source: FMC

540. These cases demonstrate that the reporting entities and the authorities are taking steps to identify assets that are linked to designated persons. Furthermore, according to the authorities, for commercial reasons Armenian banks decline to carry out transactions linked to persons designated under other international sanctions regimes implemented by OFAC and the EU, which was confirmed by the majority of banks met by the AT onsite. The fact that they are able to identify such links, despite having no legal obligation to apply EU and OFAC sanctions regimes, further demonstrates that the private sector has the necessary measures in place to enable them to identify assets linked to designated persons and therefore could identify assets linked to persons designated under the UNSCRs related to TF. The AT was therefore satisfied that the lack of any assets frozen under the relevant UNSCRs was not due to an inability of the jurisdiction to identify such links.

541. As no assets have been frozen under these UNSCRs Armenia has not received a request for access to frozen assets. It has also not received a request for unfreezing or delisting. While this is in line with Armenia's risk profile, it means that the procedures for granting access to frozen funds, unfreezing and delisting as described under R.6 have not been used in practice, although Armenia has issued guidance on these issues.

10.2. Identification and deprivation of terrorist funds or other assets

542. Armenia's legal framework enables the confiscation or forfeiture of assets and instrumentalities linked to terrorism and TF activities and the application of provisional measures, with or without a conviction. This is underpinned by investigatory powers and special investigative techniques. The competent authorities for these purposes are the FMC, the NSS, the IC and the GPO.

543. The AML/CTF/CPF National Strategy for 2022-2024 envisaged the creation of a methodology for the confiscation of assets and instrumentalities related to TF activities. This has been completed and incorporated as an appendix to the Technical Guidance on Investigation into TF Offences referred to under IO.9. However, as indicated under IO.9, this document has not yet been applied in practice, and therefore its operational effectiveness cannot be assessed.

544. Nevertheless, the GPO confirmed that in the course of the terrorism cases referred to under IO.9, property comprising instrumentalities was recovered and retained by the authorities. See the second case study under IO.9 for examples.

545. The NSS monitors international alerts about developments related to terrorist financing methods, and shares these with the other authorities to assist them in identifying assets linked to terrorists. However, to date no such assets have been identified outside the context of the terrorism cases referred to above. While this is broadly in line with Armenia's risk profile, the concern identified under IO.9 about the extent to which the authorities consider the use of criminal proceeds for TF purposes is also a relevant factor, given that limitations on the identification of terrorist financing activity inevitably restrict the identification of terrorist assets.

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

Identification of at -risk NPOs

546. As explained under R.8, in the context of the 2021- 2023 NRA, just over 1 000 entities (primarily non-governmental organisations, foundations and religious organisations) were identified as falling within the FATF definition of NPOs, and the TF risks of these NPOs were assessed as low. While Armenia identified 15 out of the 1 100 NPOs as having a higher TF risk than the others, this was relative only, as these 15 NPOs were still considered to present a low TF risk.

547. The 15 higher risk NPOs consist of 10 non-governmental organisations and five foundations. They are primarily engaged in various social, charitable, and socio-cultural programmes. Their activities focus on serving vulnerable groups in need of support, including children and vulnerable adults, displaced populations, and other at-risk communities, and funds are directed toward community development initiatives (e.g. road construction and renovation, educational and medical projects).

548. The NRA findings were supplemented by detailed analysis in a 2024 TF sectorial risk assessment, as reflected in a summary provided to the AT. Information for this assessment was obtained via a questionnaire to evaluate the TF threats to NPOs, the NPO sector's awareness of TF risks and the effectiveness of their controls and internal risk management practices. The information obtained included data on links with high-risk countries and types of transactions. Data on transactions covered a wide range of factors such as cross-border aspects (especially transactions with high-risk countries), cash withdrawals and the use of crypto-assets and alternative transfer systems. In addition to the questionnaire responses, information contained in NPO reports and open-source studies on NPOs was also considered.

549. The information obtained showed that approximately 10% of all NPOs are engaged in international transfers. Between 2021 and 2023, transfers to other countries period amounted to approximately EUR 300 million and were primarily made to Armenian diaspora communities (particularly in the Russian Federation, the United States and various European countries, especially Italy, Spain, the United Kingdom, Belgium, and France) to support social, cultural, and educational purposes. Approximately EUR 2.2 million came from the 15 higher risk NPOs. The total volume of transfers to high-risk countries was just under EUR 2 million, with just over EUR 300 000 coming from two of the 15 higher risk NPOs. These transfers were primarily made to support Armenian cultural centres and, in some cases, individual beneficiaries under humanitarian aid programmes (strictly under charitable purposes).

550. Funds received from abroad in the same period amounted to just over EUR 400 million. This was a substantial increase on funds received in the period immediately before then and was largely due to contributions from Armenian diaspora communities (primarily in the Russian Federation, the United States and European countries including Switzerland, Germany, and France).

551. Fundraising is conducted primarily through bank transfers and online donations (via POS terminals and payment systems), with no indications of NPOs collecting or distributing funds through alternative transfer systems or using crypto assets. The financial transactions of NPOs typically do not involve complex or multi-layered intermediary chains. Most funds come from international and local donors, as well as individual donors, and are allocated directly to the implementation and maintenance of programs and events.

552. According to the authorities, a key factor in the assessment of the NPO sector as low risk for TF is that the activities of Armenian NPOs almost exclusively involve funds raised by Armenians for the benefit of other Armenians, whether Armenian residents or members of the Armenian diaspora. This was demonstrated by the information on cross-border transfers referred to above and was also confirmed by the NPOs who were met onsite, all of whom were among the 15 higher risk NPOs.

553. While the overall assessment of the NPO sector as low risk for TF appears to be in line with the underlying data referenced in the sectorial risk assessment, this is not consistent with the approach taken

by the banking sector, as banks classify nearly 80% of their NPO clients as high risk. According to the authorities however, this classification is not a reliable indicator of TF risks and is primarily due to the banks taking a conservative approach for commercial reasons, as banks risk assess all NPOs, including those that do not meet the FATF definition, and classify them as high risk if they meet any one of the risk criteria. On the basis of the material provided, there was no reason to believe that the information held by the banks contradicted the overall findings of the assessment of the NPO sector as low risk.

Mitigating measures

554. As explained under R.8, there are mitigating measures in place under the AML/CFT Law which require NPOs to maintain information on domestic and international transactions, identification data about their managing officials, foundation documents and records of management decisions, and documents on their financial and economic activities. These measures are not risk based, as they apply equally to all NPOs in the jurisdiction.

555. The position is different as regards enforcement of these measures. The AML/CFT Law provides that NPO supervisors are required upon request from the FMC to take measures to prevent the involvement or usage of NPOs in ML/TF. According to the authorities, this enables the oversight and enforcement of mitigation measures in practice to be targeted at those considered to have a higher risk of TF, and Armenia has taken steps to achieve this in practice. The FMC and the SRC (as the AML/CFT supervisor for NPOs that are non-governmental organisations and foundations) have created a formal programme of supervision for the 15 higher risk NPOs, which was appended as a table to the 2024 sectorial analysis summary.

556. The table classifies three of the 15 NPOs as relatively high-risk, with annual control measures assigned, and the remaining 12 NPOs as medium level risk and subject to control measures on a two-year cycle. However, it is expressly stated that this is not static and may change over time in line with changing circumstances. In all cases, offsite supervision is envisaged.

557. While these control measures appear to be focused and proportionate to the risk profiles of the NPOs in question, their effectiveness could not be fully assessed, as formal implementation has not begun yet. However, in 2025 the SRC carried out some preparatory engagement with the 15 NPOs, following issuing of the questionnaires referred to above. Based on the responses to the questionnaires, the SRC (and also the FMC in some cases) held follow up meetings with the NPOs in 2025 to discuss any issues of concern. Overall, these meetings demonstrated that appropriate controls were in place. This was in line with the information provided by the NPOs who were met onsite, who confirmed that records were kept on management officials and on all financial and economic activities, supported, as necessary, by desk-based and onsite checks to ensure that the use of funds was consistent with the NPO's stated purposes.

558. Therefore, although there was no formal application of risk-based mitigation measures during the assessment period, some risk-based oversight of the NPO sector was introduced towards the end of the assessment period. This oversight involved reaching agreement with NPOs about the application of controls etc. rather than the authorities applying any enforcement. However, this is of limited significance in practice, given the overall finding by the authorities that appropriate controls were in place.

Box 10.2. Case Study –Targeted engagement with NPO

Following the issue of a targeted questionnaire in 2024, from the beginning of 2025 the SRC held individual meetings with representatives of NPOs identified as higher risk.

In one of these meetings the NPO confirmed that although it did not have formal programmatic provisions specifically aimed at ensuring staff awareness of TF risks, employees were nevertheless informed about potential TF risks associated both with NPOs in general and with their organization's specific activities. This awareness was raised in the context of the organization's mission, geographic areas of operation, and the processes related to the fundraising and allocation of financial resources. Employees were instructed to exercise heightened vigilance in these matters.

Certain issues were also identified regarding the regulation of internal processes, particularly those related to the collection and distribution of funds. This was observed despite the fact that, in practice, these activities are generally conducted in line with established rules. Following the recommendation of the SRC — and with its support, where necessary — the NPO agreed to develop and formalize documented procedures describing the regulated steps of these processes within a defined timeframe. As a result, an agreement was reached between the NPO and the SRC to carry out targeted work on the identified areas of concern and to fully implement the necessary steps for establishing processes that meet the required standards. The parties agreed to complete these actions within a one-year period, setting the first half of 2026 as the implementation deadline.

Source: SRC

559. Armenia has taken other measures to develop the understanding of the NPO sector about TF issues. A number of guidance documents related to the TF risks for NPOs have been published on the FMC website, and information about the findings of the NRA on this issue has been presented to the NPOs considered to be at greater risk of TF. In addition, in 2024 there was a workshop jointly organised with the CoE where the topics covered included the ways in which NPOs could be abused for TF purposes.

560. Nevertheless, and notwithstanding the guidance and outreach provided by Armenia, the NPOs that were met onsite displayed only a limited understanding of the ways in which NPOs can be abused for TF purposes. While they were generally aware of their obligations under the AML/CFT Law and had developed internal controls intended to mitigate TF risks, the limited depth of their understanding of TF abuse could affect the extent to which these controls can always be effectively applied in practice. The materiality of this is nonetheless limited, given the small number of higher risks NPOs and their risk profile, in particular their focus on Armenian residents and diaspora communities and the low volume of transfers they make to high-risk countries.

10.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

10.4.1. FIs and VASPs

561. According to the authorities, FIs are very well aware of their obligations to screen customers and transactions against lists of designated persons and have mechanisms in place for doing this. This was confirmed by the FIs met onsite, who demonstrated a good level of understanding of, and compliance with, their screening obligations. The authorities also advised that since 2022, FIs generally have made substantial investments in upgrading their sanctions screening frameworks to enhance operational efficiency and ensure timely identification of designated subjects. This has been done in response to the evolving geopolitical landscape. As regards the most commonly identified TFS shortcomings, no data was provided about this but according to the authorities, these are the same shortcomings as those identified in the thematic inspections for banks looked at below.

562. As part of the CDD and transaction monitoring processes, FIs routinely screen client names, shareholders, UBOs, authorised signatories, directors, and associated addresses. With respect to transaction screening, FIs also screen the names and addresses of the transaction originator and beneficiary, as well as any other FIs involved in the payment chain. This is always carried out at the point of customer onboarding and prior to the execution of new transactions.

563. The banking sector is the most relevant in terms of materiality and transactional volume. It uses advanced and comprehensive screening solutions, which are typically sourced from well-known global

providers. This enables screening to be conducted on a continuous basis, including by overnight batch screening of the entire customer base against the most recent updates to the UN Lists and the 1373 National List. Typically, the system will automatically block any account where a suspected sanction match has been found. Some of the larger non-bank FIs have automated screening systems similar to those of the banks. For others, screening is carried out manually.

564. The effectiveness of sanctions screening by a number of banks was assessed in thematic inspections carried out by the FSLD in 2023 and 2025 (see Core Issue 10.5 for further details). In all instances, the systems identified transactions or business relationships involving designated entities. This applied at every level within a structure, including within complex structures. The deficiencies observed were predominantly related to operational risk (e.g. institutions not retaining historical records of all listings and de-listings, issues related to audit trail in regard to resolving matches etc.).

565. These findings were in line with feedback from FIs met onsite. Banks and larger NBFIs demonstrated ability to screen through multi-layered ownership structures to the underlying natural person level. This was not an issue for smaller FIs, that generally only transact with legal persons that have simple ownership structures.

566. For those FIs that have automated systems, the continuous monitoring of their client database against UN lists and the 1373 National List means that any changes to designations are automatically picked up. Therefore, while all FIs met onsite were aware of the sanctions updates provided by the FMC and the search facility on its website, these resources are primarily relied on by smaller FIs that do not have automated systems and carry out manual searches. While these searches are usually done on the day that an update to a sanctions list is received, occasionally this may not be done until the following day. However, this not a material issue, given that the clients of smaller FIs are typically Armenian and where they are legal persons, they are not part of a complex structure and do not have foreign beneficial owners.

567. FIs are also aware of their obligation to make a report to the FMC in the event of any matches, and this has happened in practice as regards the banking sector, albeit not in relation to the TF related TFS (see under Core Issue 10.1).

568. The banks and other large FIs met onsite generally also demonstrated a good understanding of sanctions evasion. When asked how their products and services could be used to circumvent TFS, they were able to give examples of the type of activity involved in sanctions evasion in line with international typologies and identified the measures that they have in place to address this. This included looking at the use of shell companies, parties that might be acting on behalf of designated persons (e.g. associates or professional representatives such as trustees) and checking that transactions have a legitimate purpose. Understanding of sanctions evasion was less developed among smaller FIs. However, the materiality of this is limited as they typically carry out simple transactions for Armenia clients without any cross-border element. Furthermore, as indicated above, the customer base of non-bank FIs consists primarily of natural persons, with legal persons representing a negligible share (less than 0.01%). Where legal persons are present, they are predominantly characterized by simple ownership and control structures, with no apparent transparency issues, and therefore do not readily lend themselves to being abused for sanctions evasion purposes.

569. As explained under IO.3, at the time of the onsite visit there were no licensed VASPS as the regime was still being implemented, so VASPs were considered non-material for the purposes of the evaluation.

10.4.2. DNFBPs

570. According to the authorities, understanding of sanctions issues among DNFBPs is more varied than with FIs, but overall is still good. Some of the larger DNFBPs, primarily those that are part of large

international groups, use automated screening tools comparable to those used by banks and larger FIs, but most DNFBPs rely on manual screening.

571. Screening is carried out at by DNFBPs at the point of customer onboarding and prior to the execution of new transactions as part of their CDD and transaction monitoring processes, in the same way as with FIs. All of the DNFBPs met onsite were aware of their obligations in this regard and confirmed that they have processes for meeting their obligations, although some stated that they would only do this in respect of non-Armenian clients. They were also aware of their obligation to report any matches to the FMC, although to date no such matches have been reported by any DNFBPs met onsite. This is in line with the fact that, as confirmed in the NRA, most of those DNFBPs have an exclusively Armenian client base and within that, the proportion of legal persons is small.

572. As DNFBPs with automated systems that carry out continuous screening are in a minority, most DNFBPs have to carry out manual screening against updates to UN lists and the 1373 National List. All the DNFBPs met onsite were aware of the sanctions updates provided by the FMC and the search facility on its website, and confirmed that they used these resources to carry out checks. In general, this is done as soon as an update is received, but for one entity in the gambling sector, this is only done on a weekly basis. However, given the client base of that particular DNFBP (Armenian citizens or non-citizens of Armenian origin), the risk of a sanctions breach arising from that delay in this singular case is not material.

573. DNFBPs involved in cross border transactions have good awareness of sanctions evasion risks. The understanding of sanctions evasion among DNFBPs not involved in cross border transactions is less developed. However, the materiality of this is limited, given the small size of the sector and its relatively limited market footprint. This, coupled with its domestic focus, relatively low volume of transactions its generally simple transaction activity, and very limited exposure to higher risk or cross-border clients, means that DNFBPs are unlikely to be abused for sanctions evasion purposes.

10.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

10.5.1. FIs and VASPs

574. Competent authorities monitor and ensure compliance with TF-related TFS through (i) guidance and training provided to the financial sector as a whole, and (ii) supervisory engagements with individual FIs.

575. As regards guidance and training, the authorities have implemented a range of measures in this respect. The Freezing Guidance referred to under Core Issue 10.4, which has been in place throughout the assessment period, outlines freezing obligations, mechanisms for communication of listing decisions to reporting entities, guidance to parties holding frozen property and information on preventive measures to disrupt access to or use of property by persons related to terrorism. This has been recently supplemented by a “Guidance on Criteria for the high-risk and Suspicion of Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction”, which contains information about high-risk criteria and indicators of suspicion.

576. The authorities organised training events, including presentations and workshops, to further the understanding of the private sector. According to the authorities, information about TFS has been included in general AML/CFT training events that have been organised by the authorities throughout the assessment period. This has been supplemented by training events specifically focused on TFS. In January 2024 a workshop for reporting entities was organised in cooperation with representatives of the CoE. This workshop, which was attended by over 140 participants, covered the TFS risks applicable to each type of reporting entity, their obligations and duties; overview of the TFS lists, the types of

sanctions and rules; the TFS mechanisms put in place by reporting entities, ongoing monitoring and practical guidance on identifying, preventing and reporting TF. Furthermore, following feedback in December 2023 from bank representatives about their wish for more advanced training on TFS (following a training event on trade sanctions), in October 2024 the FSLD organized a specialized training program focused on UN TFS, tailored for representatives of banks, investment firms, and MVTS providers. Extracts from the materials used at the events in January 2024 and October 2024 were provided to the AT, and they demonstrated that the scope of the events was comprehensive, and the information provided was of high quality.

577. The FIs that were met onsite were familiar with the guidance provided by the authorities on TFS and had attended the training events on this topic. All confirmed that they had found the guidance and training useful.

578. As regards supervisory engagement with individual FIs, this takes the form of off- site and on-site supervision. According to the authorities, the primary source of off-site data from a TFS perspective is the annual risk assessment of FIs. In particular, from the inherent risk assessment perspective, the TF risk levels of FIs are assessed by considering exposure to countries and clients that are high risk from a TF perspective. From an internal control assessment perspective, particular attention is paid to the adequacy of automated screening systems and customer due diligence (including risk assessment) in general. The authorities confirmed that TFS implementation is always included in full-scope on-site inspections and while designing inspection plans, consideration is given to TF residual risk profiles to determine the scope of inspection from a TFS perspective.

579. Supervision has primarily focused on the banking sector, which is understandable given that it is the most material from a TFS perspective. As referred to under Core Issue 10.4, the FSLD has carried out two thematic inspections in relation to the banking sector. The first, in 2023, involved 13 banks and comprised an evaluation of internal processes and controls, followed by the use of test data to verify that screening systems could successfully detect matches with designated persons. The conclusion from the inspection was that sanctions screening solutions deployed by all inspected banks were capable of effectively identifying matches with persons and entities listed by the UN. Nonetheless, several areas for improvement were identified, particularly concerning the need for periodic testing and fine-tuning of sanctions screening software to maintain optimal performance. As a result, the FSLD issued a circular to all banks outlining supervisory expectations regarding the sanctions screening process.

580. The second thematic inspection, in 2025, involved 18 banks and was carried out in conjunction with the FMC with the aim of reaffirming and following up on the findings of the 2023 inspection. A broader and more comprehensive set of test data was employed in this round to assess system responsiveness and detection capability. The results confirmed that all banks' sanctions screening systems were able to successfully detect matches with persons and entities included in the UN Lists. While there were no cases identified of deficiencies in the screening process, there were some related deficiencies (e.g. a bank did not maintain historic records of all listings and de-listings) which resulted in specific actions by the FSLD. As a result of the inspection, a document summarising the finding of the monitoring was compiled which contained the deficiency identified and recommendation for remedying the deficiency. Primarily banks were requested to develop concise action plan for remedying deficiencies. The FSLD continues to monitor the implementation of the developed action plans.

581. In the view of the AT, these two thematic inspections are impressive, both in terms of their scope and the positive outcomes, as described above. In addition, in 2024 the FSLD carried out a full review of TFS compliance by two banks as part of a full-scope AML/CFT inspection. One of these reviews resulted in some identified deficiencies and the imposition of a sanction.

Box 10.3. Case Study – Identified Deficiency in Bank Screening Systems

During a full-scope AML/CTF/CPF inspection in December 2024, a joint FSLD- FMC team reviewed Bank's A implementation of TFS obligations.

Although Bank A had integrated a sanctions screening module into its core banking system, to screen new customer information against the UN Lists and the 1373 National List, the inspection revealed a technical deficiency in the way the screening module operates within the customer onboarding workflow.

Specifically, it was identified that the system performs sanctions screening at an early stage of the onboarding process but did not automatically re-screen customer data when it was manually edited (e.g., name or identification details) before final registration. As a result, there was a window of vulnerability during which altered customer information might be recorded into the system without being properly checked against the relevant sanctions lists. While other screening processes (e.g. transaction screening and periodic monitoring) were functional, this gap represented a compliance risk at the point of entry into the financial system, as a designated person could bypass detection if critical identifiers were changed after the initial check.

This finding was considered a breach of Article 28 of the AML/CTF Law; and was reflected in the overall supervisory sanctions that were imposed for this and other breaches (namely a formal warning, an order to eliminate violations, an administrative fine for the entity of approximately EUR 340 000 and an administrative fine for the MLRO of approximately EUR 2 300).

Source: CBA

582. As regards non-bank FIs, to date they have not been subject to any specific onsite inspections in relation to TFS. However, according to the FSLD issues of TFS compliance are considered within the context of general AML/CFT inspections (see under IO.3) and are routinely raised in the course of meetings between the FSLD and all FIs. This was confirmed by some of the FIs that were met onsite.

583. The FSLD also evaluates the adequacy of all FIs' sanctions screening frameworks offsite as part of the annual risk assessment process. This requires FIs to submit detailed information regarding the screening solutions employed and the corresponding screening procedures. This information is subsequently reviewed by the FSLD and integrated into the institution's overall risk profile. According to the authorities, any deficiencies identified during this process are communicated to the respective institutions through supervisory "Dear CEO" letters, and examples of such letters were provided.

584. No supervisory action has been taken to address possible delays in manual checks against updates to lists. However, as indicated above the risk of these delays leading to a sanctions breach is low.

585. Overall, the level of supervisory engagement of the FSLD for both banks and non-bank FIs regarding TFS appears to be in line with the risks of the sector. However, this engagement is focused very heavily on screening, with only limited coverage of the controls that FIs have in place to prevent sanctions evasion. In the view of the AT, there is scope for increased engagement on this topic, in particular in relation to typologies of sanctions evasion in TF cases.

10.5.2. DNFBPs

586. The DNFBPs met onsite were familiar with the TFS guidance issued by the authorities and almost all had attended training sessions on this topic. As with FIs, they confirmed that they had found the guidance and training useful.

587. According to the authorities, the monitoring of TFS compliance by DNFPBs primarily comprises off-site risk-based supervision, whereby DNFPBs fill-in a designated self-assessment questionnaire, which includes specific parts on the TFS framework that the entity has in place.

Following this, the questionnaires as well as DNFBPs' risk assessments are analysed and based on the results, if there are issues identified, proposals for enhancing specific processes, developing and implementing work plans, and addressing existing deficiencies are made. In terms of the identification of TFS-related infringements, a special form titled a "Protocol" is generated, which contains information on the supervision measures taken and the nature of the infringements. The DNFBP is also given a specific timeframe to report on the implementation of actions aimed at eliminating or rectifying the infringement.

588. There have been no thematic inspections of TFS compliance by DNFBPs. As regards lawyers, accountants, estate agents, and DPMS monitoring and compliance with TFS is specifically envisaged as part of general onsite and offsite supervisory engagement by provisions in the FMC's DNFBP supervisory manual. However, as explained under IO.4 no onsite inspections have been carried out to date by the FMC, although the DNFBPs that were met onsite generally confirmed that questions about their screening processes were included in questionnaires from the FMC.

589. During onsite inspections the SRC evaluates the ability of gambling operators to comply with the requirements established by AML/CFT legislation, including TFS obligations. Some of the DNFBPs supervised by the SRC that were met onsite confirmed that the SRC had carried out checks on their screening systems.

590. The level of supervisory engagement appears to be in line with the TFS risks of the DNFBP sector overall. However, as with FIs, the focus on issues related to sanctions evasion appears limited, although this is less material for most DNFBPs given their customer profiles.

591. According to the information provided by Armenia, no deficiencies have been identified in relation to TFS compliance by any DNFBP. Consequently, no enforcement action has been taken. This indicates that the supervisory activity carried out in relation to DNFBPs has not identified the instance referred to above where a DNFBP reported taking a week to make checks against changes to UN lists. Although the materiality of this is low, this is still something which the AT would expect the supervisor to have picked up and addressed to ensure that all checks are made immediately.

Chapter 11. Proliferation Financing Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Armenia has well-established mechanisms for PF policy coordination, with the Interagency Committee and FMC ensuring structured cooperation and information exchange. Operational coordination functions when required.

b) Armenia has completed two PF NRAs and demonstrated a generally sound understanding of PF risks, including links to PF-hub jurisdictions and sanctions-evasion typologies. While there are some analytical gaps in the NRA reports, particularly in relation to financial flows and the use of virtual assets for possible sanctions evasion, understanding of these issues is more developed at a practical level.

c) PF-related TFS are implemented without delay, following the same mechanisms as TF-related TFS. Armenia demonstrated its ability to identify and freeze assets promptly under the Iran PF sanctions regime.

d) All FIs and some DNFBPs have carried out PF risk assessments. Banks and larger FIs have a good understanding of PF-TFS obligations and evasions risks, while smaller FIs and DNFBPs show more limited knowledge, which is consistent with their domestic profiles and lower risk exposure.

e) The CBA monitors the risk assessments put in place by FIs. Supervisory engagement more generally mirrors the TF-TFS approach, with guidance, outreach, and inspections contributing to overall compliance, though supervisory focus on specific PF issues relating to sanctions evasion remains limited.

Key Recommended Actions (KRA)

No KRA

Other Recommended Actions

a) Armenian supervisory authorities should develop further guidance on PF sanctions evasion typologies (e.g. by reference to enhancement of the understanding of financial flows, the use of virtual assets for possible sanctions evasion, and exposure to PF hub countries) and ensure smaller FIs and DNFBPs receive tailored outreach that reflects their specific business models and risk exposure. The supervisory engagement with non-bank FIs and DNFBPs should be enhanced and its focus expanded beyond screening processes to include sanctions evasions risks and practical vulnerabilities.
b) Authorities should enhance future PF NRA reports by including greater analysis of financial flows, virtual assets and exposure to PF-hub jurisdictions to reflect their operational understanding.

Overall conclusion on IO.11

Armenia has robust systems in place for coordination and cooperation at a policy and an operational level. PF risks are understood and appropriate and mitigating measures have been put in place. TFS related to PF are implemented without delay, and assets linked to designated persons have been quickly identified and frozen. Understanding and compliance of reporting entities as regards TFS obligations is good, subject to some deficiencies which are not material from a risk perspective. The authorities take appropriate measures to monitor and ensure compliance with TFS, but more needs to be done in relation to sanctions evasion.

Armenia is rated as having a substantial level of effectiveness for IO.11.

11.1. Competent authorities co-operation and co-ordination to combat PF financing

11.1.1. Co-operation and co-ordination to develop and implement policy

592. Armenia has well established cooperation and coordination mechanisms in place for the development and implementation of CPF policy. The Interagency Committee is responsible for high-level policy making and coordination in this area, as specified in a government regulation governing the functions of the Interagency Committee relation to CPF. This regulation states that the Interagency Committee is responsible for coordinating NRAs, including the PF NRA, for both creating a coordinated national policy in the field of CPF and developing an action plan for the implementation of that policy, and for developing legal acts in the field of CPF. As explained under IO.1, the membership of the Interagency Committee includes all of the key AML/CTF/CPF stakeholder agencies, including policy makers, the FMC, LEAs, supervisors, customs and tax authorities and the judiciary. Representatives of the banking association may also attend by specific invitation. On average the Interagency Committee meets twice a year.

593. The FMC performs the role of the Secretariat to the Interagency Committee. It coordinates organizational matters, facilitates communication among members, and monitors the implementation of decisions of the Interagency Committee, reporting progress and outstanding issues to the Chairman when required.

594. The Strategic Analysis and Supervision Division of the FMC is a dedicated unit responsible for the collection and analysis of information and drafting of the PF NRA. This is done with the support of other authorities, including those having law enforcement and supervisory functions in the area of PF, as well as the private sector. The Division is adequately staffed and equipped to perform these functions.

595. To facilitate secure and efficient communication between members of Interagency Committee and FMC, a specialized system known as the Unified Information Domain was established in 2014. This platform was modernized and renamed the Financial Intelligence Data Exchange Platform in 2022. Continuous enhancements have been made to support its development, including the integration of new modules, such as a system for receiving statistical data from state institutions in 2023, and in 2024, a feedback mechanism enabling LEAs to report on the use of financial intelligence data provided by FMC. These information channels were used within the scope of the PF NRA process, for exchanging information between domestic stakeholder agencies involved. To further strengthen high-level cooperation and consensus, thematic working groups are also established.

11.1.2. Co-operation and, where appropriate, co-ordination for operational purposes

596. Measures are in place to enable cooperation and coordination for CPF operational purposes. A dedicated Working Group under the Interagency Committee provides a platform for operational level cooperation. Its members act as contact points for their respective bodies and communicate primarily through the Financial Intelligence Data Exchange Platform, which enables secure exchange of information and includes a standardized feedback module allowing LEAs to report on the use of FMC disseminations. In addition, competent authorities exchange information through the 'Mulberry' document management system.

597. Operational coordination is reinforced through joint participation in guidance and awareness raising initiatives, which routinely involve the same authorities represented in the Working Group. These activities support a shared understanding of CPF obligations and operational requirements across agencies.

598. These mechanisms are further underpinned by bilateral MoUs between the FMC and other authorities which set out the specific roles and needs of parties as well as the framework for cooperation on specified matters, including exchange of information, organization of trainings, developments of handbooks and typologies etc. This includes an MoU between the FMC and the MoE for enhancing the effectiveness of control over circulation of PF-sensitive materials and ensuring more comprehensive cooperation. Under this arrangement, the MoE regularly provides the FMC with information on licences issued for export and import of dual-use goods, as well as on licence applications that have bene refused.

599. In line with Armenia's PF risk profile described below, there has been limited need for the use of these mechanisms for CPF operational purposes. However, their effectiveness was demonstrated by actions taken by the authorities following the identification of assets linked to the Iran PF sanctions regime referred to below. An urgent meeting of the Working Group was convened, where measures were put in place to monitor the situation, to keep reporting entities informed and to remind them of their TFS obligations. The outcomes from these measures were discussed in subsequent meetings to ensure that all assets and property subject to restrictive measures were frozen without delay, and that access to property for sanctioned persons and entities was properly disrupted. In addition to this case, there have been instances where the authorities have collaborated over operational measures to identify possible PF links to the export of dual use goods.

11.2. Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

600. In 2024 Armenia completed its second PF NRA (the first having been completed in 2021), which was coordinated by the Interagency Committee and took into account FATF guidance on assessing and mitigating the risks of PF. The report concluded that the jurisdiction's residual PF risks are low. It is envisaged that this exercise will be repeated every three years.

601. As would be expected given Armenia's geographical position, particular attention was given to border controls and possible PF links to the import or export of dual use goods, as well as to the measures in place for the implementation of TFS. The report identified that the residual PF risks for all FIS and DNFBPs was low, on the basis that they had appropriate measures in place to address their inherent vulnerabilities. Nevertheless, while in the view of the AT the overall conclusions of the PF NRA appear reasonable, there are some concerns about limitations on the analysis in the PF NRA report. In particular, the threat indicators are limited and while the PF NRA report adequately analyses the risks of breach or non-implementation of TFS relating to PF, it gives insufficient consideration to financial flows and the use of virtual assets for possible sanctions evasion. In addition, while the PF NRA report takes into account its links with Iran and the fact that it has no links with the DPRK, it does not identify PF hub countries, i.e. those through which assets may be routed to Iran or the DPRK, or assess the

specific PF sanctions evasion risks presented by Armenia's links with PF hub countries, including three countries in particular.

602. However, in onsite discussions on PF risks, the authorities demonstrated a greater understanding of these issues than appeared from the PF NRA report. They were familiar with FATF typologies on sanctions evasion, both generically and in their relevance to Armenia and showed a strongly developed awareness of the PF risks arising from their geographical position. They also provided details of the extensive engagement with the international community on this and other sanctions related issues that informed their view of PF risks. The authorities further explained that strategic analysis carried out by the FMC in respect of PF risks arising from crypto-asset activity work had informed the PF NRA, and this was confirmed in written material provided after the onsite visit.

603. Authorities also demonstrated awareness of the positions and reports of several jurisdictions and international organisations depicting PF hubs generally, including the three countries in particular mentioned above. As regards two of those countries, information was provided after the onsite visit about the way in which the potential use of outbound flows to the financial institutions under the jurisdiction of those countries for PF purposes had been considered. This involved looking at a range of factors identified in international typologies including, among other things, the use of shell companies and intermediary jurisdictions (including their financial systems, primarily via correspondent relationships), revenue generation via IT workers and front companies (possibly by persons and entities associated with the DPRK), the risks associated with foreign financial institutions potentially being used to bypass the obligations stemming from TFS established by the UNSCRs, the possible misuse of outflows resulting from legitimate trade for PF or PF-related evasion schemes, the possible misuse of exported goods, the fabrication of end-user documents relating to dual-use goods, possibly including false end-use statements and repackaging concealed military applications, the risks of diversion of licensed and dual-use goods for export for potential PF or PF-related evasion schemes and the possible involvement of crypto-asset service providers and crypto-assets for PF or PF-related evasion schemes. As regards the third country, the authorities advised that the FMC had carried out specific analysis on this. Although for reasons of security the analysis itself could not be shared with the AT, a summary was made available instead, and this confirmed that the authorities had looked into flows from Armenia to that country.

604. On the basis of this additional information, the AT was satisfied that the authorities have a sufficient understanding of the PF risks faced by Armenia.

605. As regards mitigating measures, a range of measures to address PF risks have been included in the 2025-2028 National Strategy for Combating Money Laundering, Terrorism Financing and Financing of Proliferation of Weapons of Mass Destruction which was approved by the Interagency Committee in December 2024. These include measures to increase awareness of PF risks and to enhance risk-based supervision in this area. As would be expected given the time frame, some of these measures are still in progress. However, some measures have already been completed. In particular, targeted training has been organised for the authorities and the private sector, and guidance has been issued for reporting entities on red flags for PF-related targeted financial sanctions evasion schemes potentially associated with specific foreign jurisdictions that are seen as sensitive for PF purposes. According to the authorities, these are the mitigating measures which they regard as the most important.

606. The positive effect of these mitigating measures can be seen in the awareness of sanctions evasion and PF hub countries demonstrated by the banks and other reporting entities with cross border business that were met onsite (see below).

11.3. Implementation of PF-related targeted financial sanctions without delay

607. TFS related to PF are implemented in the same way as TFS for TF, both as regards the legal framework and the process for providing information about changes to designations. The analysis under Core Issue 10.1 on this issue is therefore equally applicable here.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

11.4.1. Identifying funds or assets held by designated persons/entities/persons acting on their behalf or at their direction

608. The analysis under IO.10 as regards the effectiveness of the systems in place for identification of assets linked to designated persons applies equally here.

609. The effectiveness of these systems in relation to PF in particular was demonstrated by the fact that during the assessment period there was an instance of a bank identifying and freezing funds linked to persons designated under the Iran PF sanctions regime. No assets linked to persons designated under the DPRK PF sanctions regimes have been identified, which is in line with Armenia's PF risks.

Box 11.1. Case Study – PF related asset freeze

On Saturday 27 September 2025, the UN re-established the sanctions list relating to Iran under UNSCR 1737 (i.e. so -called snapback sanctions) and published a notice about this the following day. The automated overnight sanctions screening system of an Armenian bank identified links between persons designated under these sanctions and two accounts held by the bank and put an automatic block on each account. Both accounts were with banks under a corresponding banking relationship. The first was an Iranian bank whose account with the Armenian bank was empty as it had never been used. The second was a Malaysian bank owned by an Iranian bank and its account held approximately EUR 183 000.

When the bank opened for business on the Monday morning, a report was made to the FMC. Both accounts remain frozen.

Source: FMC

11.4.2. Prohibiting financial transactions related to proliferation

610. Armenia's legal framework prohibits financial transactions that would involve dealing with the assets of a person designated under a PF sanctions regime or making funds or economic resources available to such a person. The authorities have the necessary powers and resources available to them to enable financial transactions with a PF link to be identified, and the prohibitions enforced.

611. To date there have been no instances of any financial transactions that would be captured by this prohibition. This is in line with Armenia's PF risk profile.

11.5. FIs, VASPs and DNFBPs understanding of and compliance with obligations

11.5.1. FIs and VASPs

612. The overall understanding of and compliance with TFS obligations by FIs as described under IO.10 applies equally to TFS related to PF.

613. The authorities confirmed that all FIs have PF risk assessments in place. The experience of the supervisors is that FIs generally demonstrate a sound understanding of their inherent PF risks and have implemented controls that are broadly proportionate to their size, materiality, and risk profiles. FIs largely take into account the findings of the PF NRA, although the depth and granularity of such consideration vary across sectors, reflecting their relative materiality and exposure to PF risks.

614. This was confirmed by the FIs met onsite, who generally had a good awareness of the countries that are subject to PF sanctions regimes or are PF hubs, and of the risks involved in dealing with such countries. It was confirmed that they would not generally do business with jurisdictions that are identified as high risk for PF by the FATF and would take measures (e.g. additional due diligence) to address the risks of dealing with PF hub countries.

615. As would be expected, this awareness was stronger with banks and other large FIs, who also demonstrated familiarity with FATF typologies on PF. There was less awareness of specific PF issues among the smaller FIs that were met onsite, but this is not a material concern given the nature of their customers and activities as described under IO.10.

11.5.2. DNFBPs

616. As with FIs, the overall understanding of and compliance with TFS obligations by DNFBPs as described under IO.10 applies equally to TFS related to PF.

617. The authorities advised that while some larger DNFBPs (primarily in the gambling sector) had assessed their PF risks, most DNFBPs had not. This was in line with what the AT was told by DNFBPs met onsite. Some of them had the same awareness of PF issues and the need for mitigating measures as the banks and other large FIs, but for most of them this was not the case. However, as with smaller FIs, this is not a material deficiency given the profile of those DNFBPs as described under IO.10.

11.6. Competent authorities monitoring and ensuring compliance with PF related targeted financial sanctions

618. Generally speaking, the systems for monitoring and ensuring compliance by FIs and DNFBPs with TF related TFS described under IO.10 apply equally to PF related TFS. However, the guidance described under IO.10 differentiates between TF and PF issues, and this differentiation is also applied in the course of most supervisory engagements with specific FIs and DNFBPs.

619. The CBA assesses, on an annual basis, the quality of FIs' internal control frameworks, including their approaches to identifying and mitigating PF risks. This is done through its internal risk assessment methodology. As part of this process, FIs are required to complete a risk evaluation questionnaire, which includes a dedicated section on their internal PF risk assessment. This was confirmed by copies of the questionnaires which were provided to the AT. In addition, FIs are required to submit their most recent PF risk assessment to the CBA for review.

620. As regards the DNFBPs supervised by the FMC, the annual questionnaire for evaluating ML/TF/PF risks contains specific questions requesting information on how the evaluation of the reporting entity's PF risk is being carried out, how screenings with the lists established in accordance with the relevant PF UNSCRs are carried out, the level of understanding of their TFS obligations; and the level of integration of the PF risk understanding, within their internal AML/CTF/CPF rules and procedures.

621. The SRC currently employs on-site inspections as the primary instrument for assessing PF risks. During such inspections, the ability of gambling operators to comply with the requirements established by AML/CFT legislation, including the level of sophistication of the systems and procedures designed to comply with TFS obligations stemming from the PF UNSCRs, is evaluated.

622. However, there is insufficient emphasis on sanctions evasion and the particularities in typologies for evading TFS related to PF.

Annex A. TECHNICAL COMPLIANCE ANNEX

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This analysis of technical compliance covers:

Recommendations under review:

(i) Recommendations where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated December 2015, MER 2015) or follow-up report with technical compliance re-ratings (dated July 2018, FUR 2018) – these recommendations are: **R.3, R.5, R.10, R.12, R.14, R.22, R.26, R.28, R.32, R.33, R.34 and 36;**

(ii) Recommendations where there has been a change in the FATF Standards for which the country has not previously been assessed - **R.1, R.2, R.4, R.8, R.15, R.24, R.25, R.30, R.31, R.38, R.40**. The latter Recommendations are identified with the Recommendation heading in green text.

Recommendations not under review: For Recommendations not under review, where legal, regulatory or operational framework changes introduced by the Armenian authorities were not material, no additional analysis has been conducted and mostly pre-existing information from the country's most recent assessments with technical compliance re-ratings has been compiled for inclusion in this annex. Recommendations that draw solely on MER 2015 are: R.6, R.9, R.11, R.13, R.16, R.17, R.18, R.19, R.20, R.21, R.23, R.27, R.29, R.35, R.37 and R.39. Recommendations which additionally refer to FUR 2018 are: R.7.

RECOMMENDATION 1 – ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH

In its 2015 MER, Armenia was rated PC with R.1, based on the following deficiencies: insufficient consideration of certain ML threats and vulnerabilities, impacting the proper identification and assessment of ML risks (c.1.1); no allocation of resources on a risk-sensitive basis to law enforcement and DNFBP supervisory authorities (other than the Ministry of Finance for the casino sector) to prevent or mitigate identified ML/TF risks (c.1.5); no risk assessment was used to justify the application of simplified measures (c.1.8); DNFBPs supervisors were not in a position to ensure that DNFBPs implement their obligations under R.1 (c.1.9). In its 2018 FUR, Armenia addressed most of the identified deficiencies, notably with regard to c.1.1 and 1.9, and R.1 was re-rated as LC. The FATF Standards for R.1 have undergone a revision against which the country has not previously been assessed. On this basis, R.1 is regarded as a recommendation under review (RUR).

Assessment of ML/TF risks

Criterion 1.1 – The obligation to identify and assess ML/TF risks derives from the Interagency Committee's[98] overall objectives and functions, particularly its role in coordinating the process (Interagency Committee Regulation, p.3 (1)). Armenia has completed four National Risk Assessment reports (NRA) covering the periods 2012-2014, 2014-2016, 2017-2020 and 2021-2023. Armenia has developed its own national methodology for the risk assessments which was updated for the 2023 NRA.

Criterion 1.2 – The designated authority responsible for co-ordinating actions to assess the risks is the Interagency Committee (IAC), established by decision of the Prime Minister (Decision No 45-A of 17 January 2019; Interagency Committee Regulation, p.3(1)). The IAC brings together representatives of

[98] Standing Committee on combating money laundering, terrorism financing and financing of proliferation of weapons of mass destruction in the Republic of Armenia.

competent authorities, including the FMC, supervisory and law enforcement authorities, judiciary and the banking association), and is chaired by the Governor of the Central Bank of Armenia. The FMC is responsible for collecting the information, its analysis, and drafting the risk assessment (NRA Methodology, p.6).

Criterion 1.3 – The national assessment of ML/TF risks shall be carried out regularly, once every three to four years (NRA Methodology, p.3). The IAC shall ensure that the findings of such assessments are up to date (Interagency Committee Regulation, p.3(1)). The NRAs were regularly updated with intervals of three-four years (see c.1.1).

Criterion 1.4 – The results of the NRA are fully available to member agencies of the IAC. Summaries and generally accessible versions of the reports shall be made available to reporting entities, experts and the professional community, while the main findings shall be made publicly available on the FMC's website (NRA Methodology, pp.7-8). Outreach events were organised by the FMC.

Assessment of PF risks

Criterion 1.5 – *(a)-(d)* The obligations described in c.1.1 to 1.4 extend to PF risks. The PF risks were assessed by two of the national risk assessment reports covering the periods 2017-2021 and 2021-2023.

Criterion 1.6 – The 2025 – 2028 National AML/CFT/CPF Strategy was approved by the Interagency Committee, and the implementation of the Strategy and the Action plan is being monitored semi-annually. ML action points are aligned with the ML risks and are measurable, subject to some limitations as explained under IO.1, and the few numbers of TF action points mirror the TF low residual risk. The qualitative and quantitative assessment criteria are rather general and not always linked to measurable outcomes. With regards to the Anti-Corruption Strategy for 2023-2026, more clarity in the prioritisation of the actions implementing the Anti-Corruption Strategy for 2023-2026 would be needed (see IO.1, C.I 1.2).

Measures to mitigate ML/TF risks

Criterion 1.7 – Armenia does not provide any exemptions from the FATF recommendations.

Criterion 1.8 –

(a) FIs and DNFBPs are required to apply EDD measures in high-risk scenarios established by the AML/CFT Law, the AML/CFT Minimum Requirements Regulation and the internal acts of the reporting entities (AML/CFT Law, Art 3(1)(22); RE AML/CFT Minimum Requirements, p.33). High-risk indicators are set out in Article 3(1)(21) of the AML/CFT Law and p.22 of the AML/CFT Minimum Requirements Regulation. In addition, the FMC has assessed the high-risk indicators identified in the 2021 NRA, particularly in relation to new technologies, and updated, following the 2024 NRA, the high-risk indicators in its Guideline on the criteria of high risk and the indicators of suspicious activity in relation to ML and TF. However, there is no explicit legal requirement to apply EDD measures in relation to the newly identified higher risk scenarios.

(b) There is no requirement for FIs and DNFBs to incorporate this information into their risk assessments. Nevertheless, the FMC has instructed some FIs (banks, PSPs, investment, credit and insurance companies) to take into consideration the criteria set out in the Guidance on the criteria of high risk and the indicators of suspicious activity in relation to ML and TF (FMC letter of 30 April 2021).

Criterion 1.9 – In case of low risk, the process of simplified customer due diligence may be applied, i.e., reporting entities may take lightened measures for ongoing due diligence of the business relationship (AML/CFT Law, Art.3(1)(24); RE AML/CFT Minimum Requirements, p.35). The following adhere to low-risk criteria: effectively supervised financial institutions, government bodies, local self-government bodies, state non-commercial organisations, community administrative institutions (AML/CFT Law, Art.3(1)(23)). Additionally, the Minimum Requirements for the reporting entities prescribes additional low risk scenarios: life insurance policies below certain threshold, insurance policies for pension schemes, payments relating to salaries, allowances, utility services, pensions, also payments to the state authorities (RE AML/CFT Minimum Requirements, p.28). While the low-risk scenarios are not directly deriving from the NRA, they seem to be reasonable as not high-risk scenarios could be identified in their regards.

Criterion 1.10 – FIs and DNFBPs are being supervised for compliance with the AML/CFT obligations (see c.26.1, c.28.1(c) and c.28.2), which includes the risk assessment and risk mitigation requirements set out under R.1.

Measures to mitigate PF risks

Criterion 1.11 – The 2025-2028 National AML/CFT/CPF Strategy identifies five priorities, with specific actions in relation to PF outlined under the priority on *Undertaking Effective Preventive Measures*. These actions include periodic reviews of PF risks, defining necessary actions based on these reviews, organising trainings, and developing and publishing PF-related suspicious indicators. The necessary resources have been allocated to enable the measures which are the highest priority for the jurisdiction to be taken forward already, while others are currently underway (as expected given the timeline) (see IO.11).

(a) As described in c.1.7, Armenia does not provide any exemptions from the application of certain FATF Recommendations.

(b) and (c) The results of the 2024 PF NRA indicate a low level of PF risk. REs are required to assess PF risks and have policies, controls, and procedures enabling them to effectively manage and mitigate identified risk (AML/CFT Law, Art. 4(1)). Such measures do not impact the obligations under R.7, as the simplified measures are applicable only in relation to customer due diligence measures (AML/CFT Law, Art.3(1)(24); AML/CFT Minimum Requirements Regulation, p.35).

(d) Supervisors oversee implementation of AML/CFT Law which also include PF-related requirements (Art. 29(1), AML/CFT Law).

Obligations of financial institutions and designated non-financial businesses and professions

Assessment of ML/TF risks

Criterion 1.12 **–**

(a) FIs and DNFBPs are required to identify and assess their potential and existing ML/TF risks (AML/CFT Law, Art. 4(1)). Documents and information that include findings of the assessment of potential and existing ML and TF risks should be made accessible to relevant supervisory bodies (AML/CFT Law, Art.22).

(b) When assessing ML/TF risks, reporting entities should consider all relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied (AML/CFT Law, Art.4(2)).

(c) The potential and existing ML/TF risks shall be regularly reviewed, at least once in a year (AML/CFT law, Art. 4(3)).

(d) The findings of risk assessment shall be made accessible to supervisory and other competent authorities (AML/CFT Law, Art. 22(4)).

Measures to mitigate ML/TF risks

Criterion 1.13 **–**

(a) FIs and DNFBPs are required to have policies, controls, and procedures enabling them to effectively manage and mitigate identified ML/TF risks (AML/CFT Law, Art. 4 (1), 23). These shall be approved by the senior management of the entity (AML/CFT Minimum Requirements Regulation, p.4(1)(2)(5)).

(b) The internal monitoring unit of the reporting entity is required to periodically review the implementation of the approved policies, controls and procedures and make proposals for their improvement (AML/CFT Law, Art. 25(5); AML/CFT Minimum Requirements Regulation, p.16(2)). The management body shall approve any additional measures aimed at addressing the identified shortcomings and control their implementation (AML/CFT Minimum Requirements Regulation, p.4(3)).

(c) In case of higher risks defined by the reporting entity's internal policies, enhanced customer due diligence shall be applied (AML/CFT Law, Art. 3(1)(21), Art. 18(2); AML/CFT Minimum Requirements Regulation, p.33).

Criterion 1.14 – Simplified CDD is only permitted in situations presenting a lower risk and is not allowed where high-risk criteria or suspicions of ML/FT exist (AML/CFT Law, Art. 3(1)(23), Art. 18(5)). The low-risk criteria are exhaustively defined by law and supervisory legal acts, and SDD measures based on the low-risk scenarios identified by the reporting entities are not permitted.

Assessment of PF risks and measures to mitigate them

Criterion 1.15 –

(a) FIs and DNFBPs are required to identify and assess their potential and existing ML/TF/PF risks (AML/CFT Law, Art. 4 (1)). Reporting entities are required to retain the information and documents established by law, including the findings of the risk assessments and make them accessible to supervisory and other competent authorities (AML/CFT Law, Art. 22(4)). The risks shall be reviewed regularly at intervals of not more than one year (AML/CFT Law, Art. 4(3)).

(b) Reporting entities are required to have policies, controls, and procedures enabling them to effectively manage and mitigate identified risks (AML/CFT Law, Art. 4(1), 23). These shall be approved by the senior management of the entity (AML/CFT Minimum Requirements Regulation, p.4(1)(2)(5)).

(c) The internal monitoring unit of the reporting entity is required to periodically review the implementation of the approved policies, controls and procedures and make proposals for their improvement (AML/CFT Law, Art. 25(5); AML/CFT Minimum Requirements Regulation, p.16(2)). The management body shall approve any additional measures aimed at addressing the identified shortcomings and control their implementation (AML/CFT Minimum Requirements Regulation, p.4(3)).

(d) The internal policies, controls and procedures shall enable the reporting entities to effectively manage and mitigate identified ML/TF/PF risks (Art. 4(1) AML/CFT Law). No examples of enhanced measures to be applied in order to manage and mitigate the higher PF risks are provided.

(e) The simplified measures permitted to be applied are exclusively connected to the extent of CDD (AML/CFT Law, Art. 3(1)(24), Art. 18(5)) and do not directly affect obligations regarding implementation of targeted financial sanctions and PF, in particular. The low-risk criteria are defined only by law and supervisory legal acts and cannot be established by the reporting entities (AML/CFT Law, Art. 3(1)(23)).

Weighting and Conclusion

Armenia meets or largely meets almost all of the requirements of R.1. Minor shortcomings remain: concerns regarding the general nature of some qualitative and quantitative criteria for monitoring the progress of the AML/CFT/CPF Strategy and Action Plan and a need for more clarity in the prioritisation of the actions implementing the Anti-Corruption Strategy for 2023-2026 (c.1.6); no explicit legal requirement to apply EDD measures in relation to the newly identified higher risk scenarios and no requirement to incorporate the high risk identified by the NRA into the reporting entities' risk assessment (c.1.8); the low-risk scenarios are not deriving from the NRA (c.1.9); although the obligation to adopt policies and procedures to manage and mitigate the higher PF risks is in place, no examples of enhanced measures to be applied are provided (c.1.15(d)). **Armenia is rated LC with R.1.**

RECOMMENDATION 2 – NATIONAL CO-OPERATION AND CO-ORDINATION

In its 2015 MER, Armenia was rated LC with R.2, based on the following shortcoming: the need for further development of the framework for co-operation and the co-ordination of policies on PF issues. The FATF Standards for R.2 have undergone a revision against which the country has not been previously assessed. On this basis, R.2 is regarded as a recommendation under review (RUR).

Criterion 2.1 – The 2025-2028 National Strategy for Combating ML, TF, and PF was approved on 27 December 2024 by the IAC. This was preceded by the 2022-2024 Strategy. Chapter 3 of the 2025-2028 National Strategy for Combating ML, TF and PF states that the monitoring is done on a semi-annual basis where it will be assessed to what extent the strategic tasks defined to achieve the strategic goals are implemented.

Criterion 2.2 – The IAC brings together representatives of competent authorities, including the FMC, supervisory and law enforcement authorities, judiciary and the banking association), and is chaired by the Governor of the Central Bank of Armenia, which facilitates the development and implementation of AML/CFT/CPF policies (Decision No 45-A of 17 January 2019; Interagency Committee Regulation, p.3(1)).

Criterion 2.3 – The Interagency Committee is responsible for co-ordinating the actions relation to the national risk assessment, ensuring that the findings are up to date, as well as developing a unified state policy in the field of AML/CFT/CPF (IAC Regulation, pp. 3, 4). Additionally, bilateral MoUs have been signed by the FMC with the MIA, GPO, the NSS, and the SRC.

Criterion 2.4 – Inter-agency co-operation is facilitated through the establishment of a working group under the Interagency Committee (IAC Regulation, pp. 30-35). Bilateral MoUs have been signed by the FMC with the MIA, GPO, the NSS, and the SRC to ensure exchange of information. The AML/CFT Law (Chapter 4) provides the legal framework for operational co-operation between the FMC and LEAs. This applies only when there is suspicion of ML, or TF or of a suspicion or a case of predicate offence that could lead to ML, or when such information is requested always to or from the FMC. However, there is no explicit reference to PF. Whilst Armenian authorities interpret that PF is indirectly included by referring to predicate offences, in this context, PF becomes relevant only if it leads to ML. Armenian authorities report having established Financial Intelligence Data Exchange Platform and shared data platforms. Nevertheless, there are no formal typology or intelligence-sharing mechanisms to ensure systemic operational information exchange between LEAs and intelligence bodies (see IO.1).

Criterion 2.5 – The Personal Data Protection Agency (PDPA), established in 2015, is a structural unit of the Ministry of Justice, which is represented in the Interagency Committee, thus ensuring the relevant framework for cooperation. Legal expertise, including verification of the compliance of all draft legislation with data protection rules, is ensured by the Ministry of Justice (Law on normative acts, Art. 6(2)).

Weighting and Conclusion

Armenia has in place a sound legal framework for domestic co-operation and co-ordination concerning the development and implementation of AML/CFT/CPF policies. However, minor shortcomings remain regarding the mechanisms in place for effective operational cooperation (PF and systemic operational exchange). **Armenia is LC with R.2**.

RECOMMENDATION 3 - MONEY LAUNDERING OFFENCE

In its 2015 MER, Armenia was rated LC with R.3, based on the sole technical compliance factor related to the absence of corporate criminal liability. R.3 did not undergo a follow-up review. Since then, Armenia enacted in 2021 a new Criminal Code (CC) which introduced the concept of corporate criminal liability. The new CC came into force in 2022, while the provisions on the corporate criminal liability in January 2023. These changes are considered material. On this basis, R.3 is regarded as a recommendation under review (RUR).

Criterion 3.1 – Armenia has signed and ratified both the Vienna Convention and the Palermo Convention and has generally criminalised money laundering on the basis of the relevant provisions of these international treaties (Article 296 of the CC). Nevertheless, in accordance with the interpretation of the legal framework in Armenia by the Court of Cassation decisions (EKD/0090/01/09)[99] and confirmed by jurisprudence, the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime, is not considered as money laundering. An additional element is required demonstrating the "purpose to launder". This implies the scope of the aforementioned ML offences is narrower than as defined in the Vienna Convention and Palermo Convention.

Criterion 3.2 – Armenia applies an "all crimes" approach. Under Article 296 of the CC, any criminal activity may be considered as a predicate offence for ML. The new CC includes all designated categories of offences.

Criterion 3.3 – All criminal offences may be predicate offences for ML.

Criterion 3.4 – The ML offence extends to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. The definition of the *property obtained (directly or indirectly) in a criminal way* is established by Article 121(10) of the CC (Article 296(5)). It extends to a wide range of assets, including material goods, movable or immovable objects of civil law, including financial (monetary) means, payment instruments, securities and property rights, documents or other means verifying the property rights, the interest received out of the property or interests accrued on it, the dividends or other income, as well as related rights and patent rights.

Criterion 3.5 – The recent jurisprudence (Decision of the Court of Cassation of 2021) confirms the previous interpretation of the ML offence (Decision of the Court of Cassation of 2011), concluding that it is not necessary to have a valid conviction for the predicate offence in order to establish the criminal origin of the property.

Criterion 3.6 – Predicate offences for ML extend to extraterritorial conducts (Articles 12 and 13 of the CC).

Criterion 3.7 – The ML offence applies to person who commits the predicate offence (Art. 296, CC). This interpretation has been reflected in judicial practice.

Criterion 3.8 – Intent and knowledge can be inferred from objective factual circumstances, as the judiciary shall be bound by the factual circumstances underlying the charges (Article 21(5) of the CPC) and shall examine the evidence based on the principle of the free and bona-fide assessment (Article 22(2) of the CPC).

Criterion 3.9 – The basic ML offence remains punishable for a term of imprisonment of two to five

[99] The Court of Cassation decisions are considered binding. Source: https://www.osce.org/yerevan/202596; OSCE report on selected issues regarding the admissibility of appeals to the Cassation Court of the Republic of Armenia, 2012, para 14, page 4.

years. There are some aggravating factors which may provide heavier periods of imprisonments from 5 to 12 years. The aggravating factors include committing ML by a group of persons with a prior agreement, by a criminal organization, by use of official or service powers or influence conditioned thereof or in large amounts (exceeding 5 million Armenian drams). The criminal sanctions on ML appear to be dissuasive and proportionate.

Criterion 3.10 – The criminal liability of legal persons was introduced in 2021 (in force as of January 1, 2023) and is established under Article 122 of the CC. Although the legislation does not expressly state that the liability of a legal person is without prejudice to the criminal liability of a natural person, this is implicit under Article 123(5) of the CC, which specifies that the criminal liability of a natural person does not exclude the criminal liability of the legal person for the same crime, so expressly contemplates parallel criminal proceedings for legal and natural persons. The criminal sanctions that may be applied under Article 126 of the CC are a fine of up to 20% of the legal person's gross income during the year preceding completion of the crime, temporary suspension of the right to exercise certain types of activity, compulsory liquidation and a ban on carrying out activity within the territory of Armenia. These sanctions appear proportionate and dissuasive.

Nevertheless, the scope of criminal liability of a legal person is limited, as a broad exemption apply under certain conditions. A legal person shall be released from criminal liability if it has: (i) eliminated the causes and conditions that contributed to commission of the offence, if any; (ii) compensated the caused damage and settled other consequences of the alleged crime; and (iii) returned any property acquired as a result of the offence, including the income received (Article 125(2) of the CC).

Criterion 3.11 – The CC includes the appropriate ancillary offences required under Criterion 3.11 which are covered by Articles 42-47, 50, 318 and 319 of the CC.

Weighting and Conclusion

Shortcomings remain. Not all elements of the ML offence defined in the Vienna and Palermo conventions are applicable in Armenia and there is a limited scope of corporate criminal liability (c.3.1 and c.3.10). **Armenia is PC with R.3.**

RECOMMENDATION 4 - CONFISCATION AND PROVISIONAL MEASURES

In its 2015 MER, Armenia was rated LC with R.4, based on the following deficiencies: unduly cumbersome requirements imposed by the Law on Operational Intelligence Activity (LOIA) for the deployment of certain investigative techniques which might have a restrictive impact on law enforcement authorities' ability to identify and trace property that is subject to confiscation; and the attached property was not subject to systematic management. R.4 did not undergo a follow-up review. The FATF Standards for R.4 have undergone a revision against which the country has not previously been assessed. On this basis, R.4 is regarded as a recommendation under review (RUR).

General Principles

Criterion 4.1 –

(a) The main policy frameworks addressing strategic objectives related to asset recovery are the Anti-corruption Strategies (AC) 2019-2022 and 2023-2026, and the AML/CFT/ PFT Strategy 2025-2026. The AC's Action plan for 2023 – 2026 includes actions for improving and modernising the mechanism for the confiscation of property of illicit origin, as well as to enhance the management framework for property seized, restricted, or confiscated due to corruption-related offences. Although the primary focus of the strategic objective related to asset recovery actions is criminal property associated with corruption proceeds and on improving the legal and institutions systems for combating corruption, as demonstrated by the outcomes of the previous Anti-corruption Strategy (2019-2022), the envisaged actions may have implications for the overall asset recovery system. The main achievements of the

2019-2022 Strategy include: the adoption of the Law on civil forfeiture of illegal assets (LCFIA) in 2020; the approval of the 2020 implementing Government Decision on the procedure for holding a tender for the management of property transferred to the state during confiscation proceeding; and the establishment of a new department within the GPO dedicated to the confiscation of property of illicit origin. The Action Plan for the 2025 – 2028 AML/CFT/PFS strategy emphasizes the need to enhance mechanisms for recovering and managing proceeds from corruption and property of illicit origin by identifying, imposing attachment on and confiscating the criminal property derived from predicate offences and ML, ensuring that statistical data on attachment and confiscation rates of criminal property, with a breakdown into individual predicate offences, are maintained; and ensuring effective property management. Priority actions outlined in the strategy include: (i) establishing an integrated platform to facilitate information exchange between intelligence units, investigative and prosecutorial bodies and asset recovery specialists; (ii) introducing further amendments to the legal framework on civil forfeiture; (iii) developing a methodology and guidelines for the confiscation of criminal proceeds; and (iv) Improving mutual legal assistance mechanisms to facilitate the confiscation of illegal proceeds. While the proposed activities are of significance, it is evident that most of those are still under development, and there remains uncertainty regarding the policy decision or documents that prioritise asset recovery in the country.

On the operational level, as mentioned above, following the adoption of the new legal framework on civil forfeiture of illegal assets, a specialised department for confiscation of property of illicit origin was established in 2020 within the GPO. To facilitate the international co-operation on asset recovery, Armenia became a member of the Camden Asset Recovery Inter-Agency Network (CARIN) in November 2020. However, the AT was not provided with information on other authorities with competence in asset recovery.

(b) The introduction of the civil forfeiture mechanism, its subsequent amendments of 2022, the planned actions to enhance the management framework for seizes and confiscated property related to corruption offences, indicate the asset recovery regime is subject to certain periodical reviews. The new requirements for collecting statistics on the value of seized property, imposed penalties, and the value of confiscated property are a positive development and may facilitate periodic assessments of the effectiveness of the asset recovery regime (see c. 33.1 (c)).

(c) The Strategies and their implementing action plans envisage certain actions aimed at providing adequate resources for the LEAs, are still not fully implemented.

(d) Strategic issues with regard to asset recovery system can be raised and discussed within the framework of the Interagency Committee.

Investigative measures

Criterion 4.2 –

(a)-(b) The provision of the CPC and the LOIA provide for a range of measures to identify and trace property subject to confiscation (CPC, Articles 131, 208, 209, 221-225, 234-237, 239; LOIA, Article 14). Competent authorities also have access to a wide range of investigative techniques for the investigation of ML, associated crimes and TF under the CPC and LOIA (CPC, Chapters 30, 31 on *undercover investigative actions*; LOIA, Article 14 on *types of operational intelligence* measures). However, the deficiencies identified under R.31 apply (see c.31.1-c.31.3). The available measures are subject to certain limitations, in particularly regarding the powers to use compulsory measures for the production of records held by FIs, DNFBPs and other natural or legal persons, the scope of application of the available investigative techniques, and the timely access to a wide range of information for the identification and tracing of criminal property.

Provisional measures

Criterion 4.3 –

(a) The FMC has the power to suspend a transaction or business relationship which extends to cases of suspected ML, TF or predicate offence (AML/CFT Law, 10(1)(11), Article 26(1)). The suspension can be applied based on the filed reports by the FIs, requests from foreign financial intelligence bodies, analysis of information provided by supervisory bodies and authorities involved in operational intelligence activities, as well as by public participants in proceedings, or of other information. The resolution of the FMC to suspend the transaction or business relationship should be implemented immediately upon receipt thereof by the FI. However, there is no possibility for the FMC to take such measures in the case of DNFBPs.

(b) The FMC can suspend a transaction or business relationship for period of up to 15 days. When the FMC disseminates information to LEAs, the suspension period is extended by 15 days, and may be further extended up to 30 days, if necessary (Article 26(2)(3)(3.1) of the AML/CFT Law).

Criterion 4.4 –

(a) There are available measures for the competent authorities to seize property for the purpose of securing the compensation for the possibly caused damages, the costs of proceedings, or for future confiscation of property (CPC, Article 131(1); Chapter 15 *Attachment of property*). These measures may equally be applied in relation to property of corresponding value (CPC, Article 131(3)). In addition, the competent authorities may apply securing measures provided by the Law on civil forfeiture of illegal assets (LCFIA) with regard to assets and evidence related to civil forfeiture of illegal assets (LCFIA, Articles 13-15).

(b) The initial application of seizure, during the preliminary investigation, may be made *ex parte*, based on a decision of the investigator. The decision and the supporting materials must be submitted to the competent court for approval within three days (CPC, Article (133)). The preliminary secure of evidence in civil forfeiture proceedings may be made based on a court decision, without a prior notification, with an obligation to notify the interested parties within five working days (LCFIA, Article 15(1), 16(1)).

(c) There are no unreasonable or unduly restrictive conditions hindering the effective seizure of property, as the applicable grounds for seizure are broad enough (CPC, Article 131(2)). Nevertheless, the condition described under c.4.8 and c.4.9 in relation to the value of the illicit assets is considered restrictive.

Criterion 4.5 – The competent authorities are able to seize criminal property and property of corresponding value based on a decision of the investigator. The decision and the supporting materials must be submitted to the competent court for approval within three days (CPC, Article (133)).

Criterion 4.6 – The AT was not provided with the information on the specific measures in place that would enable the competent authorities to take steps that would prevent or void actions that may prejudice the country's ability to seize or confiscate criminal property and property of corresponding value. Certain provisions of the CPC may enable the competent authorities to take such steps. Where there is *prima facie* substantial evidence that the property constitutes instrumentalities or proceeds of crime or it has been used for the commission of TF, resulted from TF, or constitutes the object of smuggling, the investigator is required to promptly seize the respective property based on their decision, subject to judicial review within three days (CPC, Article 131(2) (3)-(4)). Seizure may also be applied by the investigator when there is a reasonable assumption that the property may be alienated, concealed, damaged, destroyed, or consumed (CPC, Article 131(2) (5)).

Confiscation

Criterion 4.7 – The property, income or other type of benefits obtained directly or indirectly as a result of a crime, the instrumentalities and means used or intended to be used, the object of a crime, as well as the equivalent property, are subject to compulsory confiscation (CC, Article 121(1)(3)).

Criterion 4.8 – Civil forfeiture can be applied in relation to illegal assets acquired by a public official after assuming office if such acquisition cannot be justified by their lawful income. In such cases, the civil confiscation based on a previous conviction there are sufficient grounds to suspect based on the material of the case that these assets are in their possession and have not been forfeited upon a criminal judgement (LCFIA, Article 5(1)). However, this measure can be applied only when the value of such assets exceeds AMD 50 mil., approximatively EUR 110 400, which is considered a restrictive condition (LCFIA, Article 24(1)).

Criterion 4.9 – Measures are in place to enable the civil forfeiture of criminal property derived from serious crimes provided by the LCFIA, including ML, predicate offences and TF (LCFIA, Articles 3(1)(4), 5.) However, this civil forfeiture can be applied only when the value of the illicit assets exceeds AMD 50 mil., approximatively EUR 110 400, which is considered a restrictive condition (LCFIA, Article 24(1)).

Asset recovery and tax authorities

Criterion 4.10 – According to the authorities, there are no regulations restricting the co-operation between domestic authorities for the purpose of asset recovery. However, the AT was not provided with information regarding the existing framework and mechanism for co-operation and information sharing between the competent investigative/prosecutorial authorities and the tax authority.

Asset management, return and disposal

Criterion 4.11 – The authorities informed that the legal and institutional framework for managing seized and confiscated property is currently under development. Certain actions related to the management of criminal property in relation to corruption and illicit enrichment are planed under the 2023-2026 Anti-Corruption Strategy. Some developments have taken place in recent years, such as the adoption of a unified procedure for financial management of funds recovered in criminal proceedings, establishing a unified treasury account for such funds (Government Decision no.1922 of 2024).

The management of the seized property during the pre-trial stage is no subject to systematic management and falls under the responsibility of multiple agencies, depending on the nature of the seized property. Article 134 of the CPC regulates the manner in which the seized property should be preserved. Precious metals and stones, foreign currency and securities exceeding a certain threshold shall be transferred to the Treasury of the Republic of Armenia for retention, whereas the Armenian currency shall be paid in the deposit account of the Court that will have jurisdiction over the proceedings. Other objects (except voluminous property and real estate) shall be sealed and kept with the body that has decided to seize the property or shall be transferred to the representative of the local self-government body for retention. (CPC, 134(2)). The voluminous property shall be sealed and left with the owner or the possessor of the property or their adult family member for preservation, whereas in case of impossibility thereof, shall be transferred to the competent state body. The person responsible for preservation of the property, shall be provided with an explanation regarding the liability provided for by law for wasting, alienating, hiding or illegally transferring such property to other person, in respect of which his signature shall be taken. (CPC, 134(2)).

The management of the confiscated also falls under the responsibility of multiple agencies, depending on the nature of the confiscated property. Money and foreign currency, including payment instruments (letters of credit, payment cards, etc.), shall be transferred via the banking system to the relevant account of the state budget through the Compulsory Enforcement Service of the Ministry of Justice. Securities shall be transferred to the Ministry of Finance for sale, with the proceeds credited to the state budget, or to the State Property Management Committee for management. Precious metals, precious stones, and items made thereof shall be transferred to the Ministry of Finance to be deposited in the State Treasury. Cultural valuables shall be transferred to the Ministry of Education, Science, Culture and Sports for expert evaluation or to determine compliance with preservation standards. Other movable and immovable property shall be transferred to the Compulsory Enforcement Service or, in cases initiated by customs authorities, to the State Revenue Committee for sale via public auction The Ministry of Finance shall maintain the record (registry) of such property. Property that cannot be sold, is withdrawn from circulation, or is unsuitable for secondary use shall be destroyed with the consent of the Ministry of Economy (Government Decision no. 146-N/2010 on approving the procedure for the use, transfer, registration and destruction of confiscated property, property recognised as ownerless in favour of the state, property transferred to the state by a judge as an unacceptable gift, and property passed to the State by right of inheritance, Annex 1, points 2, 3 and 10).

The new law on civil forfeiture of illicit assets establishes a general framework for the management of assets transferred to the State's possession within the civil forfeiture proceedings. State and local self-government bodies, as well as state organisations, may act as the "competent authority" responsible for managing such assets. Where conservation of asset value is necessary, assets may be transferred to a specialised trust management. The procedure for holding a tender for the trust management of assets is to be adopted by a government decision (LCFIA, Art. 25). Perishable or movable property that requires considerable expenses for maintaining its value may be disposed by court decision (LCFIA, Art. 26).

The State Property Management Committee under the Ministry of Territorial Administration and Infrastructure of the Republic of Armenia has a role in the management of the confiscated assets.

Criterion 4.12 – The Compulsory Enforcement Service of Armenia is responsible for enforcing confiscation orders and realising the property or value subject to the confiscation order in accordance with the CEJA Law.

Criterion 4.13 – The property of bona fide third party, the property to be returned to the victim, as well as the property necessary for compensation of damages inflicted by the crime to the victim, shall not be subject to confiscation (Article 121(7) CC). When there is a dispute between the victim and the bona fide third party over the property subject to confiscation, the confiscation of that property may be performed within civil proceedings (Article 121(8) CC).

Weighting and Conclusion

Armenia has made important developments in relation to its asset recovery regime, both legislative and operational. These include the adoption of new legal provisions on seizure and confiscation, the introduction of civil forfeiture, and the establishment of a specialised department within the GPO dedicated to the confiscation of property of illicit origin. However, important deficiencies remain. The main include limitations in the available measures for identifying, tracing and evaluating criminal property, as well as in the application of the investigative measures as described under R.31; the high threshold in relation to the value of the illicit assets limits the application of extended confiscation and civil forfeiture; deficiencies in legal and institutional framework for managing seized and confiscated property. **Armenia is PC with R.4.**

RECOMMENDATION 5 - TERRORIST FINANCING OFFENCE

In its 2015 MER, Armenia was rated LC with R.5, based on the following deficiencies: the TF offence did not apply to some acts within the scope of the treaties listed in the annex of the TF Convention, and there was no criminal liability for legal persons. In its 2018 FUR, Armenia did not address the identified deficiencies and R.5 remained rated as LC. Since then, Armenia enacted in 2021 a new Criminal Code (CC) which introduced new terrorism related offences (such as Article 309 on the financing the activity of terrorist, Article 311 on creating or managing a terrorist organisation, Article 312 on the participation in a terrorist organisation), as well as the concept of corporate criminal liability. The new CC came into force in 2022, while the provisions on the corporate criminal liability in January 2023. These changes are considered material. On this basis, R.5 is regarded as a recommendation under review (RUR).

Criterion 5.1 – TF is criminalised by Article 310 of the CC. This covers the direct or indirect provision or collection of property knowing that it will be or may be used, wholly or in part, by a terrorist organisation, or an individual terrorist, or for the commission of any of various terrorism related offences at Article 308-309, 311, 315-317 of the CC. The offence of terrorism at Article 308 of the CC also includes action recognised as terrorism by international treaties ratified by Armenia, which includes all of the instruments listed in the annex to the FT Convention as required by Article 2.1 (a) of the Convention. Armenia has not ratified the 2005 Protocol to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf. This means that acts within the scope of this treaty are not covered by the TF offence as required by the definition of terrorist act in the FATF glossary. However, given that Armenia has ratified the 1988 Protocol and the additional activity covered by the 2005 Protocol would come within the definition of terrorism at Article 308 of the CC in all cases except where it affects non-civilians, this is a minor deficiency.

Criterion 5.2 – As explained above, the TF offence at Article 310 of the CC applies to the direct or indirect provision or collection of property knowing that it will be or may be used by an individual terrorist or a terrorist organisation or for commission of the offences in Article 308, 309, 311, 315, 316 or 317 of the CC. Article 310 therefore covers the provision or collection of property that is used or may be used by a terrorist organisation or an individual terrorist, without the need for a link to a specific terrorist act.

Criterion 5.3 – The travel of individuals for terrorist purposes is criminalised by Article 309 of the CC. The financing of this travel is criminalised by virtue of the inclusion of the Article 309 offence in the activities covered by the TF offence at Article 310.

Criterion 5.4 –The definition of property set out at Article 121 (10) of the CC is broadly in line with the definition of *funds* under the FATF Glossary, extending to any material goods, movable or immovable objects of civil law, including financial (monetary) means, payment instruments, securities and property rights, documents or other means verifying the property rights, the interest received out of the property or interests accrued on it, the dividends or other income, as well as related rights and patent rights. This does not explicitly cover all the elements of the definition of *funds and other assets*, such as the *economic resources* (including oil and other natural resources), *electronic or digital assets*, or assets which potentially may be used to obtain funds, goods or services. However, according to Armenia these elements comprise movable objects of civil law, which under Article 134 of the Civil Code are defined as any property which is not immovable property.

Although Article 310 does not expressly indicate whether FT offences extend to funds from a legitimate or illegitimate source, according to Armenia a broad interpretation of the term funds is to be applied, which includes both legitimate and illegitimate sources.

Criterion 5.5 – (a) and (b) Article 310 does not require that funds be actually used in order to perform or attempt a terrorist act, or that they should be linked to a specific act.

Criterion 5.6 – Intent and knowledge can be inferred from objective factual circumstances, as the judiciary shall be bound by the factual circumstances underlying the charges (Article 21(5) of the CPC) and shall examine the evidence based on the principle of the free and bona-fide assessment (Article 22(2) of the CPC).

Criterion 5.7 – Natural persons convicted of TF are subject to imprisonment from 5 to 10 years (Article 310(1) of the CC). If the offence is committed by a criminal organisation or by use of official or service powers or influence conditioned thereof, the punishment extends to 8 to 12 years imprisonment (Article 310(2) of the CC). This range of sanctions is comparable to criminal sanctions established for the offence on facilitating the activity of terrorist (Article 309 of the CC). They therefore appear to be proportionate and dissuasive.

Criterion 5.8 – The criminal liability of legal persons was introduced in 2021 (in force as of January 1, 2023) and is established under Article 122 of the CC. Although the legislation does not expressly state that the liability of a legal person is without prejudice to the criminal liability of a natural person, this is implicit under Article 123(5) of the CC, which specifies that the criminal liability of a natural person does not exclude the criminal liability of the legal person for the same crime, so expressly contemplates parallel criminal proceedings for legal and natural persons. The criminal sanctions that may be applied under Article 126 of the CC are a fine of up to 20% of the legal person's gross income during the year preceding completion of the crime, temporary suspension of the right to exercise certain types of activity, compulsory liquidation and a ban on carrying out activity within the territory of Armenia. These sanctions appear proportionate and dissuasive.

Nevertheless, the scope of criminal liability of a legal person is limited, as a broad exemption apply under certain conditions. A legal person shall be released from criminal liability if it has: (i) eliminated the causes and conditions that contributed to commission of the offence, if any; (ii) compensated the caused damage and settled other consequences of the alleged crime; and (iii) returned any property acquired as a result of the offence, including the income received (Article 125(2) of the CC).

Criterion 5.9 – Armenia has a comprehensive range of ancillary offences to the TF offence including: attempt to commit the TF offence (Articles 42 to 44 of the CC); participation as an accomplice in a TF offence (Articles 46 and 47 of the CC); organising or directing others to commit a TF offence (Articles 46 and 47 of the CC); and contributing to the commission of a TF offence (Articles 46, 47and 50 of the CC).

Criterion 5.10 – Under Article 296 of the CC, any criminal activity may be considered as a predicate offence for ML, so this would include TF.

Criterion 5.11 – Article 310 of the CC does not differentiate between cases where the person committing the TF offence is located in the same country as the relevant terrorist acts, organisations or individual terrorists and those where that person is located in a different country. Therefore, the TF offence appears to be applicable in both cases.

Weighting and Conclusion

Apart from a minor gap in the scope of the TF offence and the limited scope of corporate criminal liability, Armenia meets all criteria under Recommendation 5. **Armenia is LC with R.5.**

RECOMMENDATION 6 - TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING

In its 2015 MER, Armenia was rated as LC with R.6, mainly due to the absence of a provision which prohibits Armenian nationals or persons or entities within Armenia (other than REs) from making any funds or other assets available to designated persons and no FURs have included a rerating. Since 2015 some non-material changes have been incorporated in the national legislation. Thus, the below analysis represents a summary of 2015 MER findings.

Criterion 6.1 – In relation to designations pursuant to UNSCR 1267/1989 and 1988:

(a) The authority for proposing persons or entities to the 1267/1989 and 1988 Committee is the Ministry of Foreign Affairs.

(b) In April 2015, Armenia adopted the Rules for Proposing Persons or Entities for Designation under the Lists Published by or in Accordance with the UNSCR (the Listing Rules). Chapter 2 of these Listing Rules provides the necessary mechanisms for identifying targets for designation, based on the designation criteria set out in the UNSCRs.

(c) The grounds for proposing persons/entities for designation to the 1267/1989 and 1988 committees are the following: (1) the presence of a valid decision regarding dissolution or prohibition of activities of an entity for the involvement in terrorism or TF; (2) the presence of a valid court judgment regarding a natural person for charges of terrorism or TF; (3) designation under lists published by international organisations; (4) the presence of a valid decision or court judgement of a foreign state in relation to (1) and (2); (5) other grounds permitted by fundamental principles of the Republic of Armenia.

The grounds listed under (3) and (5) appear to be wide enough to allow designations which are not conditional upon the existence of criminal proceedings.

(d) Chapter 4 of the Listing Rules sets out the procedures for listing.

(e) If a designation is made, the authorities are required when making the designation to provide as much relevant information as possible on the proposed name; a statement of case which contains as much detail as possible on the basis for the listing; and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known (Listing Rules, chap. 4, §11).

Criterion 6.2 – In relation to designations pursuant to UNSCR 1373:

(a) The competent authority responsible for designation of persons or entities that meet the criteria for designation as stipulated in UNSCR 1373 is the CBA (AML/CFT Law Article 28(4) and 10, and the Listing Rules fully provide the relevant powers to the FMC).

(b) Part 2, Article 28(4) of the AML/CFT Law generally stipulates that the FMC has authority to "develop, review, and publish list of terrorism-related persons". Chapters 3 to 5 of the Listing Rules provide the mechanisms and procedures for identifying targets for designation pursuant to UN resolution 1373.

(c) The FMC, on its own initiative or upon the request of competent foreign bodies, shall develop, review, and publish lists of terrorism-related persons (Part 2, Article 28(4) of the AML/CFT Law). Upon receipt of a request for designation, the FMC shall within 3 business days analyse the information to identify grounds and criteria for designation. To that end, the FMC may request information from other bodies (Chapter 4, Listing Rules). In the presence of reasonable grounds or reasonable basis for designation, the Authorised Body shall within 2 business days publish information on its official website, and if possible, notify the designated person or entity.

(d) The standard of proof applied when deciding whether or not to make a designation is set out in Chapter 4 of the Listing Rules (see c.6.1(c)).

(e) Requests to foreign competent authorities to make designations under their national lists must be supported by as much relevant information as possible on the proposed name and a statement of case which contains as much detail as possible on the basis for the listing (Listing Rules, Chapter 4, §11).

Criterion 6.3 – The FMC, which is the competent authority responsible for the implementation of Article 28 of the AML/CFT Law and the Listing Rules, is empowered to request and obtain information, including information subject to secrecy, from reporting entities and state bodies, including supervisory and criminal prosecution authorities relevant for the performance of its functions, including those stipulated under c.6.3. The FMC is not required to inform a person or entity against whom a designation is being considered.

Criterion 6.4 – New designations are updated by the FMC on a daily basis (Order of the Head of FIU No. 23-14/07 from November 28, 2014). Chapter 26 of the FMC Operational Manual establishes the procedure for the dissemination of the lists of terrorism-related persons to the reporting entities. The

Armenian authorities indicated that the process is manual. Every day a staff member of the International Relations Division of the FMC checks the UN lists. In the event of amendments to the lists, a report is circulated within FMC to the IT division to update the automatic database. The FMC makes the information from the UN lists available on the website, includes that in its news release, and circulates it to banks within a timeframe of 1 - 2 days. For Resolution 1373, the situation is relatively similar, as established in Section 101, Chapter 28 of the FMC Operational Manual. Once the designation is made, Part 1 of Article 28 of the AML/CFT Law provides that the property owned or controlled, directly or indirectly, by terrorism-related persons included in the lists published by or in accordance with the UNSCRs, as well as in the lists specified by the FMC, shall be subject to freezing by customs authorities and reporting entities without delay and without prior notice to the persons involved.

Criterion 6.5 – Armenia has the following legal authorities and procedures for implementing and enforcing TFS.

(a) For Resolutions 1267/1989 and 1988, there is an obligation to freeze the property of designated persons/entities without delay and without prior notice to the persons involved. As described in the analysis for c.6.4, the relevant lists are updated on a daily basis. The same procedure apples to the list of the Authorised Body developed pursuant to Resolution 1373 (Part 1, Article 28 of the AML/CFT Law). The Guidance on Freezing of Property of Designated Persons and Entities, Chapter 2 specifies that natural and legal persons and state authorities are subject to the freezing requirement stipulated in the UNSC resolutions.

(b) The freezing obligation at Part 1, Article 28 of the AML /CFT Law extends to property that is wholly or jointly owned or controlled, directly or indirectly by the designated person or entity. It also extends to income derived or generated from such property. In addition, Part 1, Article 28 of the AML /CFT Law also specifies that the freezing obligation extends beyond funds/assets which can be tied to a particular terrorist act, plot or threat, including property owned by persons and entities acting on behalf, or at the direction, of designated persons/entities.

(c) Part 2, Article 28 of the AML /CFT Law expressly prohibits every person from making property or financial services available, wholly or partly and directly or indirectly, to persons associated with terrorism, persons owned or controlled by them or persons acting on their behalf or at their direction. In addition, the definition of "freezing of property" pursuant to Clause 37, Part 1, Article 3 of the AML/CFT Law requires the freezing for an indefinite term, a prohibition on the factual and (or) legal movement of the property directly or indirectly owned or controlled by persons associated with terrorism; this includes prohibition on direct or indirect possession, use, or disposal of the property, as well as on establishment of any business relationship (including provision of financial services) or conducting occasional transactions. The prohibition extends to natural and legal persons, and state authorities. There is no provision which prohibits Armenian nationals or persons or entities within Armenia (other than reporting entities) from making any funds or other assets available to designated persons.

(d) Armenia applies a mechanism for communicating designations to the financial sector and the DNFBPs.[100] The procedure for freezing of property is stipulated within the Guidance on Freezing of

100. Pursuant to Part 2, Article 28 of AML/CFT law, the Authorised Body shall publish lists of terrorism-related persons on the website of the Authorised Body. Section 106 of Chapter 29 of the FMC Operational Manual indicates that within 1 working day after the recommendation to add new designations to the FMC database is endorsed by the Head of the FMC, the head of the International Relations Department at FMC shall submit a draft letter for disseminating the list of terrorism-related persons to the reporting entities or for posting a relevant notice on the FMC website. The letter to the reporting entities shall be disseminated in accordance with the internal procedures of the CBA.

Property of Designated Persons and Entities.[101]

(e) Upon freezing property of terrorism-related persons, reporting entities are required to submit a suspicious transaction or business relationship report to the FMC (AML/CFT Law, Art.28(8)) If the freezing is conducted by state bodies and persons indicated in Part 1, Article 28 of the AML/CFT Law, they shall notify the Authorised Body without delay. According to Part 1, Article 7 of the AML/CFT Law, any attempted suspicious activity is also to be reported.

(f) Bona fide third parties acting in good faith are protected (AML/CFT law, Art. 28.9).

Criterion 6.6 –There are mechanisms for de-listing and unfreezing the funds/other assets of persons and entities which do not or no longer meet the criteria for designation, as described below:

(a) For 1267/1989 and 1988 designations, Armenia refers persons included in the lists of terrorism-related persons published by the UNSCRs to apply directly to the United Nations for delisting (AML/CFT Law, Art. 28.7).

(b) For 1373 designations, persons included in the lists of terrorism-related persons published by the Authorised Body (FMC) may apply to the Authorised Body (FMC) for delisting (AML/CFT Law, Art. 28(7)). On December 2, 2014, the CBA issued the "Rules for Delisting and for Unfreezing ". The rules indicate that the Authorised Body (FMC) shall notify the applicant of the outcomes of the consideration of application for delisting within one month. In the case of a rejected delisting application, the designated party may reapply to the FMC for delisting, provided that additional circumstances have emerged to indicate that the person does not or no longer meets the criteria for designation.

(c) For UNSCR 1373 designations, the procedures for the review of the designation decision before a court or other independent competent authorities are stipulated in Article 70 of the Administrative Fundamentals Law.

(d) For UNSCR 1988 designations, Armenia has referred to the procedures described in c.6.6(a), namely a designated person pursuant to UNSCR 1988 shall apply directly to the United Nations for delisting (AML/CFT Law, Art. 28(7)).

(e) For UNSCR 1267/1989 designations, Armenia maintains a website with contact information to the United Nations Office of the Ombudsperson (regarding the de-listing petitions).

(f) On December 2, 2014, the CBA issued the "Rules for Delisting of Terrorism-Related Persons Designated under the Lists Published by the Authorised Body, and for Unfreezing the Property of Terrorism-Related Persons". The rules, posted on the FMC website, specify the procedures and process to be applied when unfreezing the funds/assets of persons or entities that are inadvertently affected by a freezing mechanism (false positive).

(g) With regard to the mechanism for communicating de-listings and unfreezings to the financial sector and the DNFBPs, immediately upon taking such action, the FMC removes such applicants from the list within a two-day period, whilst reporting relevant changes on its official website. The FMC notifies the person whose property has been frozen, as well as the person or body having applied the freezing measure within a three-day period after completing the analysis, on the outcomes of the analysis. (Clauses 9, 12, and 14 of the Delisting and Unfreezing Rules).

Criterion 6.7 – Part 5 of Article 28 of the AML/CFT Law provides a mechanism for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses. The Freezing Guidance sets out

101. It was indicated in the MEQ, however, that FMC has delivered a number of seminars on the freezing obligation to financial institutions, DNFBPs and their respective supervisors and that FMC has developed and circulated an algorithm to facilitate identification and freezing of the funds and property of designated persons.

the necessary procedures.

Weighting and Conclusion

All criteria under R.6 are met, except for c.6.5 which is mostly met. There is no provision which prohibits Armenian nationals or persons or entities within Armenia (other than reporting entities) from making any funds or other assets available to designated persons. **Armenia is LC with R.6**.

RECOMMENDATION 7 – TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION

In its 2015 MER, Armenia was rated as PC with R.7, mainly due to the non-implementation of PF related TFS. In its 2018 FUR, Armenia addressed most of the identified deficiencies and R.7 was re-rated as LC. Since then, some non-material changes have been incorporated in the legislation. Thus, R.7 is not a Recommendation under review. The below analysis represents a summary of 2015 MER and 2018 FUR findings.

Criterion 7.1 – According to the authorities, the legal basis for the application of targeted financial sanctions under UNSCRs 1718, 1737 and their successor resolutions is found under Article 28 of the AML/CFT Law, which requires the freezing of property of terrorism-related persons or proliferation-related persons published by or in accordance with the UNSCRs without delay and without prior notice. The provision includes an obligation to apply freezing with regard to property owned or controlled, directly or indirectly, by persons included in the lists published by or in accordance with the UNSCRs.

Criterion 7.2 – The Ministry of Foreign Affairs is responsible for implementing TFS in this area:

(a) Reference is made to the analysis for c.6.5(a).

(b) The freezing obligations extend to all funds/other assets as described in the analysis for c.6.5(b).

(c) The law prohibits funds/other assets from being made available, directly or indirectly to or for the benefit of persons associated with proliferation of weapons of mass destruction, unless otherwise licensed authorised or notified in accordance with the relevant UN resolutions.

(d) Mechanisms for communication designations and guidance to financial institutions and DNFBPs are the same as described above in the analysis for c.6.5(d).

(e) The requirement to report frozen assets or any actions taken by financial institutions and DNFBPs are described in the analysis for c.6.5(e).

(f) The rights of bona fide third parties are protected, pursuant to Article 28(10) of the AML/CFT Law.

Criterion 7.3 – Relevant supervisory bodies are responsible for monitoring body compliance with the requirements set out in AML/CFT Law (now covering PF-related TFS obligations under Art. 28). Failure to comply results in administrative sanctions. While supervision over reporting entities for their compliance with the requirements of the AML/CFT Law is generally provided for in Article 29 of the AML/CFT Law, paragraph 2 of that provision refers to onsite inspections to review compliance with the requirements "to prevent money laundering and terrorism financing" only.

Criterion 7.4 – Armenia's law implements procedures for submitting de-listing requests to the UN Security Council in the case of designated persons and entities that no longer meet the criteria for designation:

(a) Pursuant to Part 7, Article 28 of the AML/CFT Law, any person included in the lists persons associated with the proliferation of weapons of mass destruction published by the United Nations Security Council resolutions may apply to the United Nations for delisting.

(b) The procedures to unfreeze the funds/assets of persons or entities with the same or similar name as designated persons or entities who are inadvertently affected by a freezing mechanism (false positive), are as described in the analysis for c.6.6(f).

(c) There are specific provisions for authorising access to funds or other assets, where the FMC has determined that the exemption conditions set out in Resolutions 1718 and 1737 are met, and in accordance with the procedures set out in those Resolutions (AML/CFT Law, Art.28(5)). Specific procedures as well as forms by which entities may submit their requests are provided in the Guidance on Freezing of Property of Designated Persons and Entities.

(d) The mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs, and guidance available, are as described in the analysis for c.6.6(g).

Criterion 7.5 – The addition to frozen accounts of interest, other earnings, or payments due under contracts, agreements or obligations that arose prior to the date of designation is addressed in the Guidance on Freezing of Property of Designated Persons and Entities. Payment of amounts due under contract entered into prior to designation is authorized, provided it has been determined that the contract and payment are not related to any of the items or activities prohibited under Resolution 1737.

Weighting and Conclusion

All criteria under R.7 are met, except for c.7.3 which is partly met. Supervisory authorities do not have powers to carry out onsite inspections and review compliance with the requirements PF related TFS obligations. **Armenia is LC with R.7**.

RECOMMENDATION 8 – NON-PROFIT ORGANISATIONS

In its 2015 MER Armenia was rated LC with R.8 based on the following deficiencies: no formal domestic review to identify the features and types of NPOs that are particularly at risk of being misused for FT or other form of terrorist support and no periodic reassessments of the NPO sector.

In the 2018 FUR, Armenia addressed all the identified deficiencies and R.8 was re-rated C. The FATF Standards for R.8 have undergone a revision against which the country has not previously been assessed. On this basis, R.8 is regarded as a RUR.

Criterion 8.1 –

(a) According to the 2021-2023 NRA, there are several different types of NPOs in Armenia, including non-governmental organisations, foundations, condominiums, trade unions, consumer cooperatives and religious organisations. Armenia has identified the subset of NPOs which fall within the FATF definition in the scope of NRAs. For the purposes of the assessment several sources were used, including data and statistics from competent authorities, financial and non-financial institutions, annual reports of NPOs and open-source information. As stated in the 2021- 2023 NRA, 1 100 out of 10 000 NPOs were identified as falling within the FATF definition of NPOs. These comprise non-governmental organisations (6 469), foundations (1 696) and religious organisations (62). The vast majority of these are NPOs established for the purpose of implementing public and charitable programs to implement various financial and humanitarian support projects.

(b) The TF risks of NPOs within the FATF definition have been assessed as part of the 2021- 2023 NRA. The assessment took into account the connections of NPOs' founders, beneficial owners, and authorised persons with high-risk countries based on citizenship or place of birth, as well as the nature of the NPO's activities, cross border transactions conducted by the organisations with high-risk countries, both direct and indirect (through their founders, beneficial owners, and authorised persons), including cash withdrawals, transactions involving crypto assets, and the use of alternative transfer systems. It also took into account NPOs' awareness of risks and the effectiveness of their internal risk management practices encompassing the quality of governance, financial management, project management, transparency, and self-regulation capacity. The absence of favourable conditions for terrorist activities and TF in Armenia was also considered. Only 15 NPOs (about 1.5%) were considered to be the riskiest from the point of view of TF, (10 non-governmental organisations and 5 foundations) which justify the overall conclusion of the NRA that the TF risk of the NPO sector is low.

(c) During the risk assessment process, the measures applicable to NPOs (including self-regulatory measures put in place by NPOs) were examined, including their awareness of risks and the effectiveness of their internal risk management practices as outlined above. Based on these findings, a number of additional risk mitigating measures were included in the AML/CFT/CFP National Strategy to ensure greater transparency in the NPO sector. These include organising trainings for more vulnerable NPOs on their vulnerabilities to TF abuse and risk and applying adequate measures for countering them, improving the tools available for risk-based supervision over NPOs to enhance the effectiveness of supervision over NPOs more vulnerable to TF abuse and risk (including, where necessary, through review of the guidance on risk-based supervision), and informing donors to NPOs about vulnerabilities of NPOs to TF abuse. In 2024, the FMC issued a Guidance for Donors of Non-Profit Organisations (NPOs) on Ensuring Transparency and Understanding Terrorist Financing Risks, and a Guidance on High-Risk Indicators of Terrorism Financing Abuse of Non-Profit Organisations. However, as the AML/CFT/CFP National Strategy was only adopted in December 2024, the other measures it contains had not been fully implemented at the time of the onsite visit.

Criterion 8.2 –

(a) All NPOs are required to maintain information on domestic and international transactions, identification data of their management, foundation documents and management decisions, and documents on their financial and economic activities. (AML/CFT Law, Art. 29). Legal entities must maintain and register with the State Registry their founding charter, and where a legal entity is an NPO its charter must specify the scope of its activities and objectives (Civil Code, Art. 55). The various laws governing specific types of legal entity (the Law on Public Organizations (Art. 3 and Art. 13), the Law on Foundations (Art. 15), and the Law on Religious Organizations (Art. 4 and Art. 15)) include general provisions regarding the purpose and governance of the legal entity in question which would apply to any of those entities that are NPOs.

In addition, public organisations must submit an annual report on their activities to the SRC (PO Law, Art. 24(1)) and foundations are obliged to publish annual reports on their activities (Foundation Law, Art. 39(1)). There is no equivalent obligation on NPOs that are religious organisations, as these are governed by the RO Law and there are no corresponding requirements under that law. However, this is a minor issue given that religious organisations comprise a very small proportion of NPOs overall and none are within the 15 NPOs identified as higher risk.

(b) There is a range of measures in place to raise and deepen TF awareness among NPOs. Outreach has been provided to the NPO sector by organising awareness raising and training activities for the representatives of NPOs and their supervisors on the AML/CTF legislative amendments, on a typology on TF through NPOs and criteria on FT suspicious transactions previously published by the FMC and on the outcomes of the ML/TF NRA. In 2024 the authorities and the Council of Europe organised a workshop on the Risks and Vulnerabilities of Terrorism Financing and Potential Misuse of NPOs for Terrorism Financing Purposes, which was attended by representatives from the authorities and from the NPO sector. This included information on among other things, how terrorist entities operate and fund their activities; nature of threats posed by terrorist entities to NPOs; examples of current trends; FATF Standards with respect to NPOs (including on the NPOs that fall under the FATF definition and the identification of NPOs at risk of TF); the effective measures and approaches to prevent the misuse of NPOs at a national level (registration/licensing, oversight and the implementation of RBA); and the effective measures and approaches by the NPO to prevent their misuse. Armenia has also taken measures to promote the 2016 FATF Report on Emerging Terrorist Financing Risks by translating it into Armenian, posting it on the FMC's website and circulating it among all stakeholders. The topic of

TF abuse has been integrated in the e-learning platform, which is available to reporting entities, relevant authorities and NPOs. Moreover, the availability of the UNSCR search engine has been communicated to the NPOs and their supervisors, which enables instant searches for possible matches with designated persons and entities. In addition, the FMC has issued guidance for the donor community and has reached out to donors of NPOs through awareness and educational activities.

(c) Armenia has not carried out any specific work with the NPO sector to refine and develop best practices. However, it has translated the FATF Best Practices Paper into Armenian and circulated it among NPOs. In addition, the workshop organised with the Council of Europe referred to under (b) included information on effective measures that NPOs could adopt to prevent their misuse.

(d) Under Article 4 of the Cashless Transactions Law, save where permitted by a lower threshold or exemption by law, it is prohibited to carry out transactions in cash for the sale of goods with a value of more than AMD 300 000 (approximately EUR 665), transactions relating to the disposal of property, the use of goods, the performance of works, the provision of services, the payment of passive income and the provision and receipt of loans where one party is a natural person. The same applies to payment and receipt of payment against any transaction carried out between foreign organisations and, legal or natural persons in Armenia. This includes donations. Therefore, transactions above the threshold must be carried out via regulated financial and payment channels.

Criterion 8.3 –

(a) NPOs' supervisors are required, upon request from the FMC, to take measures to prevent the involvement or usage of NPOs in AML/CFT (AML/CFT Law, Art. 29). The SRC is responsible for the oversight and monitoring of NPOs that are public organisations or foundations (Point 11 of the SRC Charter; in respect of NPOs that are public organisations: PO Law, Art. 27 and in respect of the Foundations: Foundations Law, Art. 38(1) (see under c.8.4)). The SRC has an MoU with the FMC, which includes provisions on co-operation on risk-based supervision of NPOs on the basis of the sectoral risk assessment. In particular, it is specified that the FMC and the SRC have agreed to support each other in the process of assessing the risks associated with non-profit organisations monitored by the SRS, and to implement a risk-based approach based on the results of this assessment. (FMC-SRC MOU, Clause 4(1)). The MoU also states that SRC agrees to plan and carry out inspections of non-profit organisations under its supervisory functions based on proposals from the FMC during the annual planning and implementation stages of its control operations. These inspections will focus on compliance with AML/CFT legislation and assessing risks, as well as predicting involvement in or use of money laundering or terrorist financing activities. (FMC-SRC MOU, Clause 4 (2)).

However, the SRC has no legal powers of oversight or enforcement as regards NPOs that are religious organisations. Religious organisations are subject to the RO Law. Responsibility for overseeing the activities of religious organisations rests with the Division for Religious Affairs (DRA) within the Prime Minister’s Office under a 2018 Government Decree, and under Article 23 of the RO Law the DRA may apply to the court for the dissolution of a religious organisation that violates the law. No information was provided about the scope of the obligations under the RO Law, the DRA’s oversight role or the information gathering powers available to it (other than clarification that Article 23 could be invoked to obtain information). However, this is not a significant issue given the low number and risk profile of religious organisations as outlined above.

(b) The authorities confirmed that most measures applicable under the legislation are applied to all NPOs without having regard to the specific level of TF risks. Similarly, it appears that apart from providing FMC guidance documents directly to higher risk NPOs, the same general outreach activities have been organised by the FMC and SRC for all types of NPOs, irrespective of their TF risk profiles. However, this is mitigated to some extent by the fact that the 15 NPOs identified as higher risk have participated in targeted meetings with the SRC. Therefore, focused, proportionate and risk-based measures in practice have been demonstrated to some extent.

Criterion 8.4 –

(a) As explained under c.8.3, the SRC is responsible for ensuring compliance by NPOs with the measures applicable to them. As regards NPOs that are public organisations, oversight of their compliance with the requirements of the PO Law is set out at Article 27 of the PO Law.

As regards NPOs that are foundations, in cases stipulated by law other authorised state bodies shall also conduct oversight in accordance with their competencies and the procedures established by law for inspections and investigations. With regard to religious organisations no corresponding provisions apply, but this is not a material deficiency for the reasons given above.

(b) Persons acting on behalf of public organisations and foundations are subject to administrative liability for non-compliance with the obligation to file annual activity reports (AO Code, Art. 169.18 and 169.26). This is punishable with a fine equal to fifty times the minimum wage, rising to an amount equal to two hundred times the minimum wage if the violation in question is not rectified within thirty days from the date of notification of the decision to impose a fine. The same sanctions apply to a public organisation that conducts its activities in a way that is inconsistent with its Charter objectives (AO Code, Art. 169.27). On the application of the SRC the court may suspend the activities of a public organisation for gross violations of that law (PO Law, Art 31), and the SRC may petition the court for a dissolution of a public organisation (PO Law, Art 32). If a foundation uses the income derived from the management of its endowment capital in a manner inconsistent with the annual program of the endowment capital, the SRC shall have the right to demand the payment of an amount equivalent to such income either to the donor or to the state budget (Foundation Law, Art. 38.4). Where a violation comprises a failure by a foundation to comply with the obligation to file an annual activity report within a specified time, the SRC shall file a petition with the court for the dissolution of the foundation. (Foundations Law, Art. 38). No authority has an explicit power to enforce compliance with the obligations under the AML/CFT Law described under c.8.2(a)). However, this is largely mitigated by the fact that the information required to be kept by NPOs under the AML/CFT Law is type of information that must be included in the annual reports of public organisations and foundations, and if it is not included the SRC may apply the sanctions described above. Therefore, the requirements under Article 29 of the AML/CFT law may be indirectly enforced by the SRC under the PO Law and the Foundations Law.

As explained under c.8.3, there are no sanctions applicable to NPOs that are religious organisations, but this is not a material deficiency.

Criterion 8.5 –

(a) Co-ordination and co-operation amongst competent authorities is achieved through the Interagency Committee at the policy-level. The Interagency Committee brings together competent authorities involved in the prevention of ML/FT (see under R.1), including most of those whose functions specifically relate to NPOs, and the banking association. However, it does not include the DRA, although the authorities advised that any issues would be communicated and coordinated via the Deputy Head of Staff of the Prime Minister of the Republic of Armenia, who is a member of the Interagency Committee. It also provides for a working group tasked with co-ordination/co-operation at operational level. Various memoranda of understanding between competent authorities also enable them to co-operate amongst each other. The sharing of relevant information takes place within the context of the Interagency Committee's work, as well as between the various authorities on a bilateral basis.

(b) The Investigative Committee has the necessary general investigative powers for investigating TF cases which would apply to NPOs in the same way as to any other party. The same is true of the powers of other parties with relevant functions such as the NSS and the FMC.

(c) There is nothing to hinder full access by the authorities of all relevant information on the administration and management of NPOs in the course of an investigation

(d) Suspicion that an NPO may be involved in or abused for TF purposes must be reported to the FMC by reporting entities in the same way as any other suspicion of TF. There are MoUs in place between the FMC, SRC, IC and NSS to ensure that authorities exchange information on any TF related suspicion, includes cases where NPOs are involved. However, there are no MoUs in place regarding the DRA.

Criterion 8.6 – International co-operation is provided regardless of whether the requests from foreign counterparts are related to ML, FT or other predicate offences in connection with any type of organisation or entity, including an NPO. The appropriate contact points are the FMC for information relating to a financial investigation, and the NSS and IC if the requested information relates to a criminal investigation. Information held by the SRC could be provided in response to a request for international co-operation and that this would be done through the GPO. The contact details of the relevant departments are published online and also officially communicated and regularly updated through international co-operation networks. The NSS is responsible for ensuring that the requirements and contact details for international co-operation requests are accessible, clear and transparent for international partners. This is done both through official websites, guidelines and formats, as well as through timely updates on international platforms and diplomatic channels.

Weighting and Conclusion

While Armenia has most of the measures in place that are required under R.8, the following deficiencies remain: the steps identified in the AML/CFT/CFP National Strategy to target specific risks within the NPO sector have not yet been fully implemented, the measures applicable to NPOs are not fully focused, proportionate and risk based, and the oversight and monitoring of the NPO sector is not fully focused, proportionate and risk based. There are also only very limited measures in place for NPOs that are religious organisations, but this is not a material deficiency given their number and risk profile. **Armenia is rated LC with R.8**

RECOMMENDATION 9 – FINANCIAL INSTITUTION SECRECY LAWS

In its 2015 MER, Armenia was rated C with R.9. Since then, Armenia adopted a new CPC in 2021. The changes are not considered material in the context of R.9 and thus, the below analysis represents the 2015 MER findings.

Criterion 9.1 – The AML/CFT legislation includes a range of provisions on the exchange of information between reporting entities, including financial institutions, and competent authorities. On specific requirements set out in the Criterion:

Article 5 of the AML/CFT Law requires reporting entities to submit information on ML and TF, including classified information. Article 10 of the AML/CFT Law empowers the FMC to request and obtain from reporting entities classified information for the purposes of the AML/CFT Law. Equally, the CBA has access to information subject to secrecy held by all financial institutions (Paragraphs 530 to 533 of the 3rd MER). With regards to the LEA's powers to access information, this is covered by the provisions of Article 29 of the LOIA in combination with the provisions of Article 209(4) and 239(4) of the Criminal Procedure Code (see the analysis of R.31).

Sharing of information between competent authorities, domestically and internationally, is ensured through Articles 10, 13 and 14 of the AML/CFT Law. The FMC, under Article 10 of the AML/CFT Law, has powers to request from "state bodies, including supervisory and criminal prosecution authorities' information (including documents) relevant for the purposes of this Law, including classified information as defined by the law". According to Article 13 of the AML/CFT Law, within a period of 10 days, the FMC is required to provide information to criminal prosecution authorities upon their request, provided that "the request contains sufficient substantiation of a suspicion or a case of ML or TF". With respect to international co-operation, under Article 14 of the AML/CFT Law, the FMC can request or exchange classified information with foreign FIUs based on bilateral agreements or commitments and ensure adequate level of confidentiality of information and limited use of information for combating ML and TF purposes.

Article 14 of the LBS allows banks to exchange or provide information on their customers "even if it represents bank secrecy" with each other or credit organisations. Banks should reject requests for obtaining information representing bank secrecy in cases when it contradicts provisions of the LBS.

According to Article 117 of the Law on Insurance, the insurers, reinsurers, insurance intermediaries may exchange or provide each other with information on their customers even in cases when it represents an insurance secret. Insurance, reinsurers and insurance intermediaries are required to decline the requests for obtaining information constituting an insurance secret if it contradicts the provisions of the Law on insurance.

There are no legislative provisions which hinder the sharing of information between financial institutions as required under R.13, 16 or 17.

Weighting and Conclusion

Financial institution secrecy does not inhibit the ability of the FMC, CBA or LEAs from accessing information they require to properly perform their functions. The sharing of information between competent authorities, domestically and internationally is not limited by financial secrecy. Equally, financial institutions may share information where this is required by R.13, 16 or 17. **Armenia is C with R.9**.

RECOMMENDATION 10 – CUSTOMER DUE DILIGENCE

In its 2015 MER Armenia was rated LC with R.10 based on the following deficiencies: no separate definition of the beneficial owner of trusts and legal arrangements in the AML/CFT Law (c.10.11), no CDD requirements for beneficiaries of life insurance and other investment related insurance policies (c.10.12) and no obligation to refrain from pursing the CDD process (and file an STR instead) in cases where a suspicion of ML/FT is formed and it is reasonably believed that the performance of the CDD process will tip-off the customer (c.10.20). R.10 did not undergo a follow-up review. Since then, Armenia amended the AML/CFT Law to address those issues, together with new provisions relating to trusts and other legal arrangements and BO identification. These changes are considered material. On this basis, R.10 is regarded as recommendation under review.

Criterion 10.1 – FIs are prohibited to open, issue, provide or serve anonymous accounts or accounts in fictitious names (AML/CFT Law, Art. 15(1)).

Criterion 10.2 – FIs are required to undertake CDD when (AML/CFT Law Art. 16(2)):

(a) Establishing a business relationship.

(b) and (c) Carrying out an occasional transaction (or linked occasional transactions), including domestic or international wire transfers, at an amount equal or above the 400-fold of the minimum salary (approximately EUR 900) unless stricter provisions are established by legislation. However, the definition of linked transactions is limited to transactions with the same party, having similar nature and occurring within 24 hours which significantly limits the scope of the provision. (AML/CFT Law, Art. 3(1) (11)).

(d) Suspicions arise with regard to ML/FT. There is no exemption or threshold that applies in this scenario.

(e) Suspicions arise with regard to the veracity or adequacy of previously obtained customer identification data (including documents).

Criterion 10.3 – FIs shall identify the customers and verify their identity using reliable and valid documents and other relevant data issued by competent authorities (AML/CFT Law, Art. 16 (4)). The customer is defined as person establishing or making use of an established business relationship, as well as the person which requests the RE to conduct, or conducts, an occasional transaction (AML/CFT Law, Art. 3(1) point 13). Although the definition of customer does not clearly differentiate between natural and legal persons and legal arrangements, this is inferred from other articles in the law. The identity of natural persons is verified based on official identity documents and for legal persons based on state registration document or other official documents including the required information (AML/CFT Law, Art. 16(4), points 1 – 3).

Criterion 10.4 – CDD includes identifying and verifying the identity of the customer, including that of any authorised person (AML/CFT Law, Art. 3(19)(a)). An "authorised person" is the one empowered by the order and on behalf of the customer, to conduct a transaction or to take certain legal or factual actions in a business relationship, including the authorisation to represent the customer through a power of attorney or in any other manner stipulated by law. (AML/CFT Law Art. 3 (15)). FIs are required to establish whether any authorised person exists, identify such person and verify his identity using reliable and valid documents issued by competent authorities and verify the authority to act on behalf of the customer (AML/CFT Law, Art. 16(5)(1)).

Criterion 10.5 – FIs are required to identify BOs and undertake reasonable measures to verify the identity of the beneficial owner, using reliable source information (AML/CFT Law, Art. 16(5)(2). Although, there is no explicit requirement for FIs to satisfy themselves that they know who the BO is, this can be inferred from the general obligation to identify and verify the BO and from the definition of the BO (for more information on the BO of a legal person/legal arrangement refer to the analysis of c.10.10 and c.10.11).

Criterion 10.6 – FIs are required to understand the customer's business profiles, the purpose and intended nature of the business relationship, and upon necessity, obtain information on the purpose and intended nature of the business relationship (AML/CFT Law, Art. 16(7)). The business profile includes information on the nature, impact, and significance of a customer's activities; the existing and expected dynamics, volumes, and areas of business relationships and occasional transactions; the existence, identity and interrelations of authorised persons and BOs; as well as other facts and circumstances regarding the customer's activities (AML/CFT Law, Art. 3(1)(17)).

Criterion 10.7 –FIs are required to conduct ongoing due diligence throughout the whole course of the business relationship, which shall include:

(a) the scrutiny of transactions to ensure that they are consistent with the information on the customer, its business and risk profile, the comparability of the customer's activities with that knowledge, including, where necessary, the source of funds (AML/CFT Law, Art.17(1)).

(b) Periodic update of the information collected under the customer due diligence process (including enhanced or simplified) to ensure that the information is kept up-to-date and relevant. The data reviews periodicity shall be determined by each reporting entity, within the following limits: (i) it must be conducted at least once a year for the information obtained for the customer identification and identify verification (AML/CFT Law, Art. 17(2)), (ii) for the other customer information, reviews shall be conducted at least once a year in case of medium risk, once in six months for higher risk and once in two years in case of lower risks (Regulation on Minimum AML/CFT requirements, §38).

Criterion 10.8 –FIs are required to understand the business profile of the customer which includes the nature, impact and significance of a customer's activity and the interrelations of authorised persons and beneficial owners (AML/CFT Law, Art. 16(7) and Art. 3(1)(17)). FIs are also required to have complete information on the powers of participants and management bodies (as opposed to understanding the ownership and control structure of customers that are legal persons, which includes trusts and legal arrangements. (AML/CFT Law, Art. 3(16) and Art. 16(6)).

Criterion 10.9 –The definition of legal person includes organizations with legal person status under Armenian and foreign law, and trust or other similar legal arrangement. Trust is further defined as a foreign legal arrangement (AML/CFT Law, Art. 3(16) & (16.1)). Unless it is specifically indicated that certain requirements apply only to the organizations with the status of legal person, all provisions applicable to legal person apply to trusts and legal arrangements as well.

For customers that are legal persons, which includes trusts and other legal arrangements as mentioned above, FIs must identify and verify the customer's identity through the following information:

(a) Legal person's name, identification number and if available, the tax identification number. There is no express requirement to obtain information on the legal form, although the charter or similar document which include information on legal form is mandatory. FIs are required to obtain that information based on the state registration document or other official documents which might be used as a proof of existence (AML/CFT Law, Art. 16(4)(2)). However, for foreign legal persons or arrangements, the legal form is not always evident from the name or registration documents, and the law does not expressly require FIs to obtain and document this information.

(b) Charter or similar document which includes information on the powers that regulate and bind the legal person, executive officers' name and surname, which refers to all members of the management body (AML/CFT Law, Art. 16(4)(2)).

(c) Registered office and the place of business, where it differs from the registered office (AML/CFT Law, Art. 16(4)(2)).

Criterion 10.10 – For customers that are legal persons, FIs are required to identify and verify the identity of the BO (AML/CFT Law, Art. 16(5)(2)). BO is the natural person who ultimately (de facto) owns the legal person customer, or ultimately (de facto) controls the customer, or on behalf of whom the transaction is being conducted. (AML/CFT Law, Art. 3(14)).

The BO of legal persons shall be the natural person who: (a) directly or indirectly holds 20% or more of the voting rights or participation in the capital of the legal person; and (b) ultimately (de facto) exercises control over the legal person through other means; or (c) where no natural person is identified by application of criteria (a) or (b) above, then the BO is the official carrying out the overall or routine management of the legal person. (AML/CFT Law, Art. 3(14)).

The legal definition does not cover combined ownerships *i.e.* situations where two or more natural persons might control jointly a legal person by voting rights or other means, although in the guidance issued by CBA this situation is covered and partly mitigates the gap (BO Guidance, §17). FIs are required to apply criteria (a) and (b) simultaneously, which goes beyond the cascading approach of c.10 (a) and (b) (AML/CFT Law, Art. 3(14), BO Guidance, §14). Therefore, it implies that all natural persons falling under (a) and (b) should be identified.

Criterion 10.11 – In case of customers that are trusts or similar legal arrangements, FIs are required to identify the BO and undertake reasonable measures to verify the BO identity, using reliable source information (AML/CFT Law, Art. 16(5)(2)).

(a) The BO of a trust shall be the settlor, trustee, beneficiary (including class of beneficiaries) protector (if any) and other natural persons exercising ultimate (de facto) control (AML/CFT Law, Art. 3(1)(14)). For beneficiaries of trust that are designated by characteristics or by class, there is no requirement for FIs to obtain sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout or when beneficiary intends to exercise the vested rights.

(b) The BO of a legal arrangement shall be persons performing equivalent or similar functions to those mentioned in case of trusts (AML/CFT Law, Art. 3(1)(14))

Criterion 10.12 – In case of life insurance or other investment related insurance contract or policies, as soon as the beneficiaries are identified or designated by characteristics, FIs should:

(a) for beneficiaries that are identified as natural or legal persons or legal arrangements, at least taking the name, surname or company name of that person (AML/CFT Law, Art. 18(4.1)(1)).

(b) for beneficiaries that are designated by characteristics or by class or on another ground, at least obtaining sufficient information that will enable to establish the identity of the beneficiaries at the time of the payout. (AML/CFT Law, Art. 18(4.1)(2)).

(c) FIs are required to conduct verification of the identity at the time of the payout (AML/CFT Law, Art. 18 (4.1)).

Criterion 10.13 – Beneficiaries of life insurance policies are considered a high-risk criterion (Art. 3(1)(21), AML/CFT Law) and these scenarios are subject to EDD. In the presence of high-risk criterion, FIs are required to take reasonable measures to identify and verify the identity of the BO of the legal person that is the beneficiary (AML/CFT Law, Art. 18(4.1)(3)).

Criterion 10.14 – FIs may only establish a business relationship or conduct an occasional transaction with a customer after obtaining identification information on the customer and verifying the customer's identity. Customer verification may be carried out in the course of establishing the business relationship or conducting the occasional transaction, or thereafter within a reasonable timeframe not exceeding 7 days, provided that the risk is effectively managed and that this is essential not to interrupt the normal conduct of business relationships with the customer (AML/CFT Law, Art 16(1)).

Criterion 10.15 – FIs shall develop and apply a policy for managing risks associated with cases of verification of identity of the customer (including BO) after establishing a business relationship, which includes at least the conditions under which the customer may conduct transactions (AML/CFT Law, Art. 18(3.1)).

Criterion 10.16 – FIs are required to conduct CDD with respect to existing customers, at appropriate intervals and in relevant cases, on the basis of materiality and risk pertinent to such customers (AML/CFT Law, Art. 18(6)). Although there is no explicit requirement, when performing CDD, to take into account whether and when CDD measures have been previously undertaken and the adequacy of data obtained, the frequency of updating the CDD information should be no less than once a year. (AML/CFT Law Art. 17(2)). Additionally, when any new legislation or new requirement comes into force, FIs are required to apply the new due diligence measures to their existing customers as soon as a transaction is conducted after the new legislation has come into force or, in the absence of such a transaction, when the customer's documentation is updated as part of ongoing due diligence measures (Regulation on Minimum AML/CFT Requirements, clause 38).

Criterion 10.17 – FIs are required to conduct enhanced CDD when high risk criteria are identified. (AML Law, Art. 18 (2)).

The high-risk criteria are defined by the law as criteria which indicate a high likelihood of ML/FT (AML/CFT Law, Art. 3(1)(21)) and include:

- specific higher-risk cases provided for by the law and regulations adopted by the CBA, which covers PEPs, who are potential or existing customers or beneficial owners; beneficiaries of life insurance policies; persons (including financial institutions) which are domiciled or reside in or are from non-compliant countries or territories; all complex or unusual large transactions, or unusual transactions or business relationships which have no apparent economic or other lawful purpose (AML/CFT Law, Art. 3(1)(21)), and;

- additional higher risk cases defined by FIs in their internal policies (AML/CFT Law, Art. 3(1)(21); Regulation on Minimum AML/CFT Requirements, clause 21).

FI are required to apply the following enhanced CDD measures, in addition to standard CDD, at a minimum: (i) obtain the senior management approval for the establishment of a business relationship, taking necessary measures to establish the source of funds and wealth of the customer, examining the background and purpose of a transaction or business relationship and conducting enhanced ongoing monitoring for PEPs (AML/CFT Law, Art. 3(1)(22)); (ii) apply so called "advanced measures" *i.e.* the collect of additional information or document to ascertain veracity and reliability of information or documents provided by the customer [and as longer as possible or several comparable reviewed periods of time, when collating sources movements, and volumes of the funds circulated through different transactions] (Regulation on Minimum AML/CFT Requirements, clauses 33 and 34).

Criterion 10.18 – FIs are permitted to conduct simplified CDD where low risk criteria exist, except if high risk criteria and suspicions of ML/FT exist (AML/CFT Law, Art.18(5)). Low risk criteria are criteria which indicate a low likelihood of ML/FT. They are exhaustively defined by law or legal acts of the CBA and include the following: (i) appropriately supervised financial institutions effectively supervised for compliance with AML/CFT requirements, (ii) government bodies, state-owned non-commercial organisations, public administration institutions (community administrative institutions) except for the bodies or organisations domiciled in non-compliant countries or territories, certain low risk life insurance policies, (iii) insurance policies for pension schemes, (iv) payments to state or community budgets, payments for utility services and (v) payments related to the provision of salaries, pensions or allowances from known sources (AML/CFT Law, Art. 3(1)(23) and Regulation on Minimum AML/CFT Requirements, clause 28).

An analysis conducted by the FMC indicated that low-risk criteria are consistent with the risks identified in the national ML/TF risk assessment. On the other hand, the limited list of the criteria restricts the application of the risk-based approach by FIs as the identification of other low risk criteria based on FI individual risk assessment is not encouraged. SDD are defined as a limited application of customer due diligence, whereby the FI may conduct reduced measures of ongoing due diligence on a business relationship defined by the legal acts of the CBA (AML/CFT Law, Art. 3(1)(24)). FIs may apply so called "lightened measures" for ongoing due diligence of the business relationship (Regulation on Minimum AML/CFT Requirements, clauses 35 and 36). See c.1.9 for more information.

Criterion 10.19 – (a) Where FIs are unable to comply with due diligence requirements, they are prohibited from executing the transaction and establishing or continuing the business relationship. If this relationship has already been established, FIs must terminate it. (b) In addition, the FI must consider submitted an STR to the financial intelligence unit (AML/CFT Law, Art. 27(1) and Art. 27(2)).

Criterion 10.20 – FIs may not conduct CDD, except for identification and verification of identity, in cases where there are suspicions of ML/TF and the FI reasonably believes that CDD may tip-off the customer. In cases where CDD cannot be performed, FIs are also required to submit an STR. (AML/CFT Law Art. 16(9)).

Weighting and conclusions

Armenia is compliant with most requirements under R.10. Nevertheless, some minor deficiencies still exist, including: (i) no explicit obligation for FIs to apply CDD measures as to satisfy themselves they know who the BO is; (ii) no requirement for FIs to understand the ownership and control structure of customers that are legal persons; (iii) no specific provision for BO identification for situations in which beneficiaries of a trust are designated by characteristics or by class; and (iv) SDD measures are not clearly defined and have very limited application. **Armenia is LC with R.10.**

RECOMMENDATION 11 – RECORD-KEEPING

In its 2015 MER, Armenia was rated C with R.11. Since then, Armenia did not amend the legislation. Thus, the below analysis represents a summary of 2015 MER findings.

Criterion 11.1 – REs are required to maintain records on transactions or business relationships, both domestic and international, including the name, the registration address (if available) and the place of residence of the customer (and the other party to the transaction), the nature, date, amount, and currency of transaction and, if available, type and number of accounts. Records on transactions are required to be kept for at 5 years from the termination of the business relationship or the completion of the transaction (Art. 22(1)(2) AML/CFT Law).

Criterion 11.2 – REs are required to maintain customer identification data, including the data on the account number and turnover, as well as business correspondence data, records on business relationships (as explained in the analysis for c.11.1), information on suspicious transactions or business relationships, as well as information concerning the process of review (analysis) and findings on transactions or business relationships recognised as suspicious, the findings of the assessment of potential and existing ML/FT risks and records on wire transfers. Such records shall be maintained for at least 5 years from the termination of the business relationship or the completion of the transaction (Art. 22(1)(2) AML/CFT Law).

Criterion 11.3 – REs are required to maintain all necessary records on transactions which would be sufficient to permit full reconstruction of individual transactions (Art. 22(1) 1) AML/CFT Law).

Criterion 11.4 – Information maintained by REs should be sufficient to enable submission of comprehensive and complete data on customers, transactions or business relationships whenever requested by the CBA or, in cases established by law, by authorities involved in operational intelligence activities, as well as by public participants in proceedings. Information should be made accessible to relevant supervisory authorities and authorities involved in operational intelligence activities, to public participants in proceedings, on a timely basis (Art. 22(3)(4) AML/CFT Law).

Weighting and Conclusion

Armenia is C with R.11.

RECOMMENDATION 12 – POLITICALLY EXPOSED PERSONS

In its 2015 MER Armenia was rated PC with R.12 based on the following deficiencies: absence of legal provision regarding domestic PEPs and persons who are or have been entrusted with a prominent function by an international organisation, as well as their family members and associates, no provisions concerning PEP beneficiaries of life insurance policies.

In 2018 FUR, Armenia did not address the identified deficiencies and R.12 remained rated as PC. Since then, Armenia amended the definition of PEPs. These changes are considered material, thus, R.12 is regarded as recommendation under review.

Criterion 12.1 –PEP is defined as an individual who is a former or present high-level public official entrusted with prominent public, political, or social functions, as well as an official who has been entrusted with prominent functions by an international organisation (AML/CFT Law, Art. 3(25)), without distinction between foreign or domestic PEPs.

All PEPs who are potential, existing customers or beneficial owners are a high-risk criterion (AML/CFT Law, Art. 23(11)). FIs are therefore required to apply the following measures:

(a) have internal controls establishing procedures for effective risk management to identify whether customer or BO is a PEP (AML/CFT Law, Art. 23(11));

(b) conduct enhanced due diligence, which includes obtaining senior management approval to establish a business relationship with the customer, to continue the business relationship when the customer or the BO is subsequently found to be a PEP (AML/CFT Law, Art. 3(22)(a) and Art. 18(2));

(c) take necessary measures to establish the source of funds and wealth of the customer, or the BO who is a PEP (AML/CFT Law, Art. 3 (22)(b) and Art. 18(2));

(d) the obligation to conduct enhanced ongoing monitoring of relationships with politically exposed persons, (AML/CFT Law, Art. 3(22.d) and Art. 18(2)).

Criterion 12.2 – (a) Legal requirements discussed under c.12.1 are equally applicable to all types of PEPs. (b) For domestic PEPs, secondary legislation limits the application of requirements under c.12.1 (b) to (d) to higher risk scenarios only (FMC Explanatory Note on PEPs).

Criterion 12.3 – Family members and close associates of PEPs are also considered to be PEPs, and therefore the same provisions described in c.12.1 and c.12.2 apply to them (AML/CFT Law, Art. 3(25)).[102]

The concept of family member is set out in an exhaustive list in the legislation, but it excludes minors (AML/CFT Law, Art. 3(25.2), Banking Law, Art. 8(4)). Though the concept of close associate is not specified in the legislation, the FMC has developed guidance for defining and identifying close associates applicable to all FIs and drawing on relevant FATF publications (FMC Explanatory Note on PEPs).

Criterion 12.4 – FIs must take reasonable measures to establish whether the customer and the BO, as well as the beneficiary of the life insurance policy or its BO, are PEPs, at the time of the pay-out (AML/CFT Law, Art. 18(2.1) and Art. 18(4.1)). When a high-risk criterion is identified for the beneficiary of the life insurance policy or its BO, FIs are obliged to apply EDD measures, including senior management approval to establish or continue the business relationship (AML/CFT Law, Art. 3(22) and Art. 18(2)). This does not clearly extend to informing senior management before the payout of the policy proceeds nor to explicitly considering making an STR.

Weighting and Conclusion

Armenia has safeguards in place to prevent PEPs from abusing the financial system. Some minor deficiencies remain regarding beneficiaries of life insurance policies (or their BOs) which are PEPs. Nevertheless, this was not given too much weight as, although the legal framework is in place, there are no life insurance providers licensed in Armenia so far. **Armenia is rated LC with R.12.**

RECOMMENDATION 13 – CORRESPONDENT BANKING

In its 2015 MER, Armenia was rated C with R.13. Since then, Armenia did not amend the legislation and the below analysis represents a summary of 2015 MER findings.

Criterion 13.1 – Pursuant to Article 19 of the AML/CFT Law, in relation to correspondent or other similar relations with foreign financial institutions, FIs are required to apply the following measures, in addition to the CDD requirements:

- Gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and, based on publicly available and other available information,

102 The wording in the legislation is ambiguous regarding whether the definition of "family members and close associates" applies to all categories of PEPs or only to officials entrusted with prominent functions by an international organisation, as it states: "***Politically exposed person*** shall be an individual, who is a former or present high- level public official entrusted with prominent public, political, or social functions, as well as an official entrusted with prominent functions by an international organization (including his or her family members or close associates). However, this ambiguity appears to result from translation, and it was confirmed during the onsite that the provision is intended to apply to all types of PEPs (AML/CFT Law; Art. 3(25)).

determine the reputation of the respondent institution and the quality of its supervision, including whether it has been or is subject to a criminal investigation or other proceeding related to ML or TF.

- Assess the respondent institutions procedures for combating ML and TF to ascertain that they are adequate and effective.
- Obtain the approval of the senior management before establishing correspondent or other similar relationships.
- Document the respective responsibilities of each institution with regard to combating ML and TF, if such responsibilities are not apparently known.

Criterion 13.2 – With respect to "payable-through accounts", under Article 19(1)(5)(a) of the AML/CFT Law, FIs are required to ascertain that the respondent institution has conducted due diligence on customers having direct access to the accounts of the correspondent and is in a position to provide, upon request, relevant data regarding the due diligence on these customers.

Criterion 13.3 – According to Article 19(2) of the AML/CFT Law, FIs are prohibited from entering into, or continuing, correspondent or other similar relations with shell banks. In addition to that, FIs are required to ascertain that, in connection with payable-through accounts, the respondent institution does not permit the accounts to be used by shell banks (AML/CFT Law, Art. 19(1)(5)(b)).

Weighting and Conclusion

Armenia is C with R.13.

RECOMMENDATION 14 – MONEY OR VALUE TRANSFER SERVICES

In its 2015 MER, Armenia was rated as C with R.14. Since then, according to the information provided by the country, no relevant material changes have been made to Armenian legislation. Whilst authorities assessed the changes as not material, the AT is of the view that the legislative changes related to the criminal sanctions (see c.14.2) for entrepreneurial activities without special permit (licence) are material as they may affect the dissuasiveness and proportionality of the sanctioning regime. Further, authorisation and application of dissuasive sanctions for carrying out unauthorised activities is a precondition to fulfil c.14.3, 14.4 and 14.5. On this basis, the legislative changes are considered material by the AT and R.14 is proposed to be regarded as a RUR.

Criterion 14.1 – Armenian legislation requires that any legal person providing MVTS services be licensed by the CBA as a payment and settlement organisation (PSO) (LPSSO, Art. 19(1) and Licencing Law, Art. 43). The types of PSO licenses include, inter alia: (a) carrying out money transfers, and (b) processing and clearing of payment instruments and settlement documents. This licensing requirement also applies to postal communication operators when providing postal money transfer services (Law on Postal Communication, Art. 11). The CBA maintains a public register of issued licences (Licencing Law, Art. 4(4)).

The provision of payment and settlement services without a respective license shall be prohibited, except for cases prescribed by the Law, that refer to the operations performed by the Central Bank and the Central Treasury of Armenia. (LPSSO, Art. 19(4)).

Criterion 14.2 – There is a dedicated division within the CBA tasked with identifying unlicensed activity regarding money or value transfer services. When such activity is discovered in practice, LEAs are notified.

Sanctions for carrying out activities without the licence are presenting limited dissuasiveness (except when a crime was carried out by a criminal organisation or caused particularly large-scale damage); and the CC provides a significant exemption from the criminal liability.

Proportionality: Carrying out MVTS activities without a licence is punishable by alternative sanctions:

a fine in the amount of ten-fold to thirty-fold to minimum salary rate (approximatively from EUR 1 660 up to EUR 5 000), or public works for a term of one hundred to two hundred hours, or restriction of liberty for a term of maximum three years, or short-term imprisonment for a term of maximum two months, or imprisonment for a term of maximum three years. The mentioned act, which was committed by a criminal organisation, or caused particularly large-scale property damage is punished by restriction of liberty for a term of one to three years, or short-term imprisonment for a term of one to two months, or imprisonment for a term of two to five years. The broad spectrum of sanctions ensures the ability of authorities to impose proportionate measures (CC, Art. 281).

Dissuasiveness: An exemption from the criminal liability is granted in the CC: a person who carried out unauthorised activities shall be exempted from criminal liability, if he/she has fully compensated the property damage caused by the crime and calculated penalties (CC, Art. 281(4)). Therefore, although proportionality is achieved, dissuasiveness is not fully reached.

Criterion 14.3 – MVTS providers are subject to the requirements of the AML/CFT Law (AML/CFT Law, Art. 3(4)(d)). The CBA is the designated exclusive supervisor for PSOs, including for monitoring AML/CFT compliance (LPSSO, Art. 24(1) and AML/CFT Law, Art. 29(1)).

Criterion 14.4 – Although there is no specific prohibition to carry out activities through agents, an MVTS cannot delegate performance of any part of its payment and settlement services to another entity, and this requirement is equivalent to a prohibition of provision of payment and settlement services through agents (LPSSO, Art. 19.1). Armenian legislation does not contain any definition of agents as articulated in the FATF general glossary, thus providing for an indirect exclusion of this type of activity. MVTS providers can perform their activities through branch offices and representations which are required to be registered according to the procedures determined by the CBA. CBA also maintains the registers of all operating branches (LPSSO, Art. 21).

Criterion 14.5 – This criterion is not applicable, as Armenia does not allow for MVTS providers to use agents.

Weighting and Conclusion

Armenia has legal framework in place to ensure compliance by MVTS with the AML/CFT requirements. Nevertheless, some deficiencies remain, such as the limited dissuasiveness of sanctions. **Armenia is rated LC with R.14.**

RECOMMENDATION 15 – NEW TECHNOLOGIES

In its 2015 MER, Armenia was rated C with R.15. The FATF Standards for R.15 have undergone a revision against which the country has not previously been assessed. On this basis, R.15 is regarded as a RUR.

Armenian legislation uses the terms “crypto-assets” and “crypto-asset service providers” to refer to what the FATF standard defines as virtual assets (VAs) and virtual asset service providers (VASPs). For purposes of this report, the FATF terminology is adopted throughout.

Criterion 15.1 – FIs are required to identify and assess potential and existing risks, which may arise in relation to the development of new products and new business practices, and the use of new or developing technologies (AML/CTF Law, Art.4(4)). However, FIs are not specifically required to identify and assess ML/TF risks that may arise in relation to new delivery mechanism.

Within the scope of the 2024 NRA, Armenia assessed to some extent the ML/TF risks derived from the use of new technologies, including new products and delivery channels in the context of emerging ML methods and trends.

Criterion 15.2 – (a) FIs are required to identify and assess potential and existing ML and TF risks, prior to the launch of new products or business practices, or the use of new or developing technologies. (Art. 4(5), AML/CFT Law). (b) FIs should have policies, controls and procedures, which enable them to effectively manage and mitigate identified risks (Art. 4(1) AML/CFT Law).

Criterion 15.3 –

(a) ML and TF risks emerging from virtual-assets (VAs) and VASPs activities are addressed in 2021 and 2024 NRAs, although there is no dedicated section on VAs, and no overall residual ML/ TF risk for this type of asset or service provider has been assessed. PF risks are assessed in the two iterations of the PF risk assessment. The 2023 PF risk assessment notes the absence of identified cases of VA misuse for PF purposes and, on this basis, assesses PF vulnerability as low. However, neither the PF risks assessments nor the 2024 NRA clearly articulate the residual PF risk related to VA or VASPs activities and operations, both focusing primarily on identified vulnerabilities rather than on an overall residual risk conclusion. Following the 2024 NRA, the FMC conducted a dedicated strategic analysis on VA-related ML/TF/PF risks, combining STR analysis, FIU and LEA intelligence, financial-flow screening, and on-chain analysis of resident VASPs. This analysis did not identify PF exposure or links to sanctioned entities and similarly assessed PF risk from VA activities as low. The analysis also assessed TF risks from VA activities as low (see IO.1 for a more detailed description of deficiencies in the analysis).

(b) and (c) VASPs are required to take steps to identify, assess, manage and mitigate their ML, TF and PF risks, as required by c.1.12, c.1.13 and c.1.14. The following deficiency identified in R.1 has an impact here: reduced (simplified) measures are not explicitly prescribed (c.1.14).

Criterion 15.4 - Virtual assets are defined as property that has a value or attests to a right that can be transferred and stored exclusively electronically, using the distributed ledger technology (DLT) or similar technology (Crypto-Asset Law, Art. 3(1) point 5).

The virtual asset services provided by the law are: (i) operation of a trading platform for VAs; (ii) custody of VAs; (iii) carrying out purchase and sale of VAs on own behalf; (iv) carrying out purchase and sale of VAs on behalf of the client; (v) reception and transmission of orders for VA transactions; (vi) placement of VAs; (vii) VA portfolio management; (viii) provision of advice on VAs; (ix) transfer of VAs; (x) issuance of asset-reference tokens.

(a)

(i) A virtual asset service provider is a legal company (limited liability or as joint stock) having obtained a license from the CBA for providing VA services in the RA, or a person having an authorisation to carry out activities of a branch in the territory of Armenia (Crypto-Asset Law, Art. 17(2)). Direct or indirect offer or provision of VA services without the licence, is prohibited. (Crypto-Asset Law, Art. 17(1)) A foreign company may directly or indirectly offer or provide VA services in the territory of the Republic of Armenia exclusively through the establishment of a subsidiary or branch, upon obtaining an authorization from the CBA (Crypto-Asset Law, Art. 21 and Art. 22(1)). Banks and PSOs, may provide some VA services without obtaining a special authorization, such as issuance of an electronic money token and services related to it. They cannot provide other types of services related to VAs. Other types of FIs, such as fund managers, investment companies, market operator or central depository are permitted to offer only certain types of services related to VAs, and only upon obtaining the relevant authorisation from the CBA in the general manner described by the law (Crypto-Asset Law, Art. 18(2) and Art. 68).

(ii) Only legal persons can be VASPs in Armenia. Natural persons cannot acquire the status of VASP in Armenia.

(b) A person or a person affiliated thereto, that intends to acquire a qualifying holding in the authorised capital of a VASP must obtain the prior consent of the CBA (Crypto-Asset Law, Art. 28(1)). Qualifying investor shall be the person meeting the specific criteria provided by the Securities Law (Crypto-Asset Law, Art. 3(1) point 30, see c.26.3).

CBA *may* (therefore not mandatory) reject the application if the person that acquires a qualifying holding (i) has been convicted for an intentionally committed crime, or (ii) has conviction that has not been expunged or cancelled, or (iii) may not substantiate the lawfulness of the means used for the acquisition (Crypto-Asset Law, Art. 29 (1), Points 3 and 4).

Executive officers of a VASP and of a foreign company shall be the chairperson and the members of the board of directors (supervisory board) (in case of forming a board), the head and the members of the executive body, the head and the members of the internal audit, as well as other persons declared as executive officers upon regulatory legal acts prescribed by the CBA (Crypto-Asset Law, Art. 34(1)). Although the MLRO is not explicitly listed in the Crypto-Asset Law, the position is considered part of senior management under the AML/CFT Law (see c.18.1). Persons that have been convicted for an intentionally committed crime that has not been expunged or cancelled, cannot be executives of a VASP (Crypto-Asset Law, Art. 34(4) point 2). In addition, Art. 34(4)(5) extends suitability restrictions to affiliated persons and empowers the CBA to disqualify a candidate due to an affiliate's prior conduct where it indicates unsuitability, including risks of mismanagement, financial deterioration, or reputational harm.

Criterion 15.5 – The Crypto-Asset Law has been adopted shortly before onsite. Under the "grandfathering rule", persons already providing virtual asset services when the law entered into force must register and obtain a license from CBA within one year after the CBA issues the relevant regulatory acts on licensing.

Apart from this exception, offering virtual asset service without a proper license is a criminal offence. (Licensing Law, Art. 43(2) point 14; CC, Art. 281). Also, the SRC can undertake administrative action in relation to such conduct (as per Art. 244^2 and 169^{14} of the Code on Administrative Offences). A dedicated division within the CBA is tasked with identifying unlicensed activity across all reporting entities, including VASPs. Detection relies on both external referrals (e.g., consumer complaints, reports from licensed institutions and tips from LEAs), and the CBA's own proactive surveillance, which includes systematic monitoring of social media, analysis of online content and the use of market intelligence tools.

Criterion 15.6 –

(a) VASPs are supervised for AML/CFT compliance by the CBA, except for service providers for operation of crypto-assets trading platforms (AML/CFT Law, Art. 3 (1) point 4 (i1) and Art. 29 (1), CBA Law, Art. 39(1), Crypto-Asset Law, Art. 82(1)). Given that the law had just entered into force, there was no regulatory or procedural framework to ensure the risk-based approach at the time of the assessment.

(b) Provisions of R.27 apply accordingly, as VASPs are considered FIs. Non-compliance with AML/CFT legal requirements or internal legal acts adopted by VASPs shall be sanctioned in accordance with the specific law, respectively the Crypto-Asset Law (AML/CFT Law, Art. 29(1) and Art. 30(2)) This comprises of a wide range of sanctions, including warnings, fines, removal of executive officer, repealing the license or termination of authorization or registration. (AML/CFT Law, Art. 30(2), Crypto-Asset Law, Art. 83(1)).

Criterion 15.7 – The authorities have amended the Guidance on Criteria of High Risk and Indicators of Suspicious Activity in Relation to ML/TF to add indicators (red flags) concerning transactions involving virtual assets. There are no further guidelines established for VASPs concerning the application of national measures to combat ML/TF.

Criterion 15.8 –

(a) and (b) – There is a large range of sanctions available to the CBA, to impose on VASPs in case they violate legal acts regulating the market in virtual assets, thus AML/CFT regulations (Crypto Asset Law, Art. 83(1))- see c.15.6.

Sanctions can be applied in relation to both legal and natural persons. CBA may apply a fine of up to 300% of the profit or loss generated as a result of the violation. If such estimation is not possible then the fine can be up to 15% of the annual revenue or income of the legal person or up to 20 000-fold of the minimum salary (approximately EUR 45 000) for natural persons, based on methodology that is to be developed and that should take into account, among others, the nature of the violation, the size of the damage caused or income generated by, or previous violations of the same person. This approach is considered proportionate and dissuasive (Crypto-Assets Law, Art. 85). The CBA may concurrently apply more than one sanction for each violation as well as issue an assignment on eliminating the underlying violation or adopting measures for prevention (AML/CFT Law, Art. 30(2), Crypto-Asset Law, Art. 83(1)-(3)).

Criterion 15.9 –

VASPs, with the exception of those providing services for operation of a crypto-asset trading platform, are considered financial institutions by the AML/CFT Law and therefore all requirements of R.10-R.21 apply to them accordingly, including identified shortcomings (AML/CFT Law, Art. 3(1)(4)(i1)).

(a) CDD is performed when carrying out an occasional transaction (including linked occasional transactions), including domestic or international wire transfers, at an amount equal or above the 400-fold of the minimum salary (approximately EUR 900) unless stricter provisions are established by legislation (AML/CFT Law Art. 16(2)):

(b) in case of transfer of virtual assets, the ordering and beneficiary institution:

(i) and (ii) should obtain and retain the name and surname or company name of both originator and beneficiary, the addresses of the decentralised ledger or VA account numbers used by originator and beneficiary, and the originator's/beneficiary's ID data, or address or date and place of birth/identification number, or domicile (AML/CFT Law, Art. 21.1(1) – (3)). The required information has to be transferred immediately and securely to the beneficiary financial institution. For VA transfers above EUR 900, CDD requirements apply, ensuring verification and accuracy of data (AML/CFT Law, Art. 16(2)). Information should be made available to competent authorities, upon request (AML/CFT Law, Art. 22(3) and (4)).

(iii) other requirements of R.16 apply accordingly to VA transfers (AML/CFT Law, Art. 21.1). Intermediary and beneficiary VASPs are required to have effective risk-based policies and procedures to identify VA transfers lacking the required information, and to reject or suspend the transfer in such cases. VASPs have also record keeping obligations applicable to all their transactions (AML/CFT Law, Art. 22(1)).

TFS obligations apply to VASPs in the same manner as to any other REs, therefore the analysis and identified deficiencies under R.6 and R.7 apply to them respectively.

(iv) legal provisions relating to transfer of virtual assets apply to all FIs providing such services, including VASPs (AML/CFT Law, Art. 20.1). Nevertheless, except for investment companies, traditional FIs authorised in Armenia cannot offer VA transfer services (Crypto-Asset Law, Art. 16(1) and Art. 18(1)).

Criterion 15.10 **–** Analysis of R.6 and R.7, including identified deficiencies, applies to VASPs in the same manner as to all other REs. Please refer to analysis of criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) as they apply to VASPs.

Criterion 15.11 - The international cooperation measures and exchange of information described in R.37 to R.40 apply to activities related to VAs or concerning VASPs.

Weighting and Conclusion

The virtual asset sector is regulated by comprehensive legal provisions. Some deficiencies remain: Armenia has assessed the ML/TF risks derived from the use of new technologies only to some extent, and no comprehensive assessment of overall residual ML/ TF risk for VA or VASPs has been conducted. **Armenia is LC with R.15**.

RECOMMENDATION 16 – WIRE TRANSFERS

In its 2015 MER, Armenia was rated C with R.16. Since then, Armenia amended the legislation to extend the threshold for the application of obligations to reject transfer orders with missing information. However, those changes are not considered material and R.16 is not regarded as a recommendation under review (RUR). Thus, the below analysis represents a summary of 2015 MER findings and includes limited changes to reflect the new legislation.

Criterion 16.1 – Article 20(1) of the AML/CFT Law requires ordering financial institutions to obtain, retain and include in the payment order accompanying the transfer the following information, for all transfers, indifferent of their value: a) forename and surname or company name of the originator and the beneficiary of the transfer; b) account numbers of the originator and the beneficiary of the transfer (or the unique reference number accompanying the transfer, where an account is not used). For wire transfers exceeding 400-fold of the minimum salary (approximately EUR 900) (with regard to the originator of the transfer: originator's identification document data, or address, or date and place of birth for natural persons, or individual identification number (state registration, individual record number, etc.), or domicile for legal persons. For wire transfer exceeding 400-fold minimum salary (EUR 900), CDD is compulsory, therefore includes verification of data to ensure accuracy (AML/CFT Law, Art. 16(2), see c.10.2).

Criterion 16.2 – Where more than one wire transfers are bundled in a batch file, under Article 20, Part 2 of the AML/CFT Law, the ordering financial institution "may choose to include in each individual transfer only the originator information (account numbers of the originator and the beneficiary of the transfer or, in the absence thereof, the unique reference number accompanying the transfer), provided that the batch file contains full information required (forename and surname or company name of the originator and the beneficiary of the transfer; account numbers of the originator and the beneficiary of the transfer (or, in the absence thereof, the unique reference number accompanying the transfer); with regard to the originator of the transfer, details of the identification document for natural persons or individual identification number (state registration, individual record number etc.) for legal persons)".

Criterion 16.3 – All cross-border wire transfers, irrespective of their value, have to be accompanied by originator and beneficiary information set out in c.16.1 (AML/CFT Law, Art. 20(1) points 1 &2).

Criterion 16.4 – REs are required to undertake CDD measures when the ML or TF suspicions arise (AML/CFT Law, Art. 16(2) point 3). REs are required to conduct verification of the customers "using reliable and valid documents issued by competent authorities and other relevant data" (AML/CFT Law, Art. 16(4)).

Criterion 16.5 – Similar provisions mentioned in c.16.1 apply to domestic transfers as well. (Art. 20, AML/CFT Law).

Criterion 16.6 – The AML/CFT Law does not permit the provision of information accompanying wire transfers by other means (other than those required under Article 20 of the AML/CFT Law). With respect to the LEAs access to the wire transfer information, REs are required to maintain information and documents specified under Article 20 of the AML/CFT Law, i.e. c.16.1 and 16.2, and make this information (including documents) accessible to the FMC and LEAs on a timely basis (as opposed to a maximum of three business days or immediately) (AML/CFT Law, Art. 22(3)).

Criterion 16.7 – REs are required to maintain information and documents obtained in the course of CDD regardless of whether the transaction or business relationship is ongoing or terminated. This requirement includes information obtained with respect to obligations related to wire transfers (Article 20 of the AML/CFT Law). In addition to that, under Article 22, Parts 2-4 of the AML/CFT Law, reporting entities are obliged to maintain information (including documents) obtained through CDD and transaction information for at least 5 years, and to enable submission of comprehensive and complete data on customers, transactions, business relationships whenever requested or in cases established by the law, to the FMC and LEAs (Article 22(3) of the AML/CFT Law).

Criterion 16.8 –Ordering FI should refuse any wire transfer which lack the information specified in Article 20 of the AML/CFT Law and should consider them as suspicious (AML/CFT Law, Art. 27(3)).

Criterion 16.9 – Under Article 20, Part 3 of the AML/CFT Law all intermediary FIs involved in the processing of a wire transfers, are required to ensure that the information accompanying a wire transfer is transmitted with the transfer.

Criterion 16.10 – Where technical limitations prevent the intermediary FI from transmitting the information accompanying a cross-border wire transfer with a related domestic wire transfer, according to Article 20(3) of the AML/CFT Law, the intermediary FI should "maintain that information in the manner and timeframes established by the AML/CFT law". As mentioned above, FIs are required to keep the information (including documents) for at least 5 years following the termination of the business relationship or completion of the transaction.

Criterion 16.11 and Criterion 16.12 – Article 20, Part 5 of the AML/CFT Law establishes the obligation for intermediary and beneficiary FIs to "adopt effective risk-based policies and procedures for identifying and taking relevant measures (including refusal or suspension) with regard to wire transfers that lack the information specified in c.16.1. In addition to that, FIs are required to consider terminating correspondent or other similar relationships with the FIs involved in the wire transfer.

Criterion 16.13 – See the analysis for c.16.11.

Criterion 16.14 – Under Article 16 of the AML/CFT Law, reporting entities are required to undertake CDD measures when carrying out domestic/international wire transfers at an amount equal or above 400-fold minimum salary (approximately EUR 1 000); this includes measures on identification and verification the identity of the customer (including that of the authorised person and the beneficial owner). In addition, under Article 22 of the AML/CFT Law reporting entities must maintain information (including documents) received in the course of the CDD for at least 5 years following the termination of the business relationship or completion of the transaction.

Criterion 16.15 – See the analysis for c.16.11.

Criterion 16.16 – Pursuant to Article 3 of the AML/CFT Law, MVTS providers defined as entities engaged in money (currency) transfer services are reporting entities, to which all requirements of the AML/CFT Law apply.

Criterion 16.17 – MVTS fall within the scope of the AML/CFT law, which contains general requirements on recognition of potential suspicious transactions and filing STRs.

Criterion 16.18 – Under Article 28, Part 1 of the AML/CFT Law reporting entities are obliged to freeze without delay and without prior notice to the person involved the property owned or controlled, directly or indirectly, by terrorism related persons included in the lists published by or in accordance with the UNSCR, as well as in the lists specified by the authorised body.

Weighting and Conclusion

Armenia is C with R.16.

RECOMMENDATION 17 – RELIANCE ON THIRD PARTIES

In its 2015 MER, Armenia was rated C with R.17. Since then, no relevant material changes have been made to Armenian legislation. Thus, the below analysis represents a summary of 2015 MER findings.

Criterion 17.1 *–*The AML/CFT Law sets out the conditions in which a reporting entity, when applying measures on identification and verification of the customer's identity and on understanding the purpose and intended nature of the business relationship, may rely on information obtained through customer due diligence undertaken by a third party. The ultimate responsibility for CDD measures remains with the RE (Article 16 of the AML/CFT Law). On the specific elements set out in the criterion, under Article 16 of the AML/CFT Law, REs are required:

- To immediately obtain the following information: a) on customer identification and verification; b) establish whether the customer is acting on behalf and (or) for the benefit of another person; c) information on the ownership and control structure of the legal person; d) establish the business profile of the customer, purpose and intended nature of the business relationship; e) establish business profile of the customer.
- To take adequate steps to satisfy themselves that the third party "is authorised and has the capacity to provide, immediately upon request, the information obtained through due diligence, including the copies of documents" and that the third party "is subject to proper regulation and supervision in terms of combatting ML and TF, as well as having effective procedures to conduct CDD and to maintain relevant information", as provided for under the AML/CFT legislation.

Criterion 17.2 – Article 16 of the AML/CFT Law requires RE to take adequate steps to satisfy themselves that the third party "is not domiciled or residing in or is not from a non-compliant country or territory". Furthermore, Article 3(1) (26) of the same law defines a non-compliant country or territory as "a foreign country or territory that, according to the lists published by the Authorised Body, is in non-compliance or improper compliance with the international requirements on combating money laundering and terrorism financing".

Criterion 17.3 – FIs are required to apply the same measures when relying on a third party that is part of the same financial group.

Weighting and Conclusion

Armenia is C with R.17.

RECOMMENDATION 18 – INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

In its 2015 MER, Armenia was rated as C with R.18. In 2017, the interpretative note to R.18 was revised to clarify the requirements on sharing of information related to unusual or suspicious transactions within financial groups. In its 2018 FUR, Armenia was considered compliant with the new requirements and the rating remained the same. Since then, no relevant material changes have been made to the legislation. The below analysis represents a summary of 2015 MER and 2018 FUR findings.

Criterion 18.1 – Article 23 of the AML/CFT Law requires FIs and other reporting entities to have in place and apply internal legal statutes (policies, concept papers, rules, regulations, procedures, instructions or other means) aimed at the prevention of ML and TF, which have regard to the size and nature of the reporting entity's activities and pertinent risks. The internal legal statutes are required to establish, at minimum, requirements on procedures for CDD, internal audit, requirements on hiring, training and professional development of the staff, procedures for effective risk management and other

AML/CFT obligations. On the specific elements set out in the criterion:

Compliance management arrangements – REs are obliged to have an internal monitoring unit, and its staff members are required to have appropriate qualification according to the criteria defined by the FMC (Article 24 of the AML/CFT Law). The *Internal monitoring unit* is defined under Article 3 (1) (29) of the AML/CFT Law as a division or employee of the reporting entity performing the function of preventing ML and TF as provided for under the AML/CFT Law and the legal statutes of the FMC. The definition of the internal monitoring unit also states that the reporting entities may delegate the functions of the internal monitoring unit to a specialised professional entity in cases and manner established by the FMC. Article 24 of the AML/CFT Law further requires internal monitoring unit to be independent and have the status of senior management of the reporting entity; and to have direct and timely access to the information (including documents) obtained and maintained under the AML/CFT Law. *Senior management*, under Article 3 (1) (28) of the AML/CFT Law, is defined as a body or employee of the reporting entity authorised to make decisions and take actions on behalf of the reporting entity on AML/CFT matters.

Screening procedures – Article 24 of the AML/CFT Law addresses internal monitoring unit of reporting entities. Part 2 of this Article states that Internal monitoring unit staff members "should have appropriate qualification awarded on the basis of qualification competence criteria defined by the Authorised Body". In addition, Article 23 (1) (9) of the AML/CFT Law requires reporting entities to adopt internal legal statutes, which should establish requirements with regard to hiring of the staff members of the internal monitoring unit and other employees in connection with the obligations defined by the AML/CFT legislation and other legal statutes.

Ongoing employee training – Article 23 (1) (9) of the AML/CFT Law requires reporting entities to establish requirements with regard to training and professional development of the staff members of the internal monitoring unit and other employees performing obligations defined by the AML/CFT legislation and other legal statutes, as well as in connection with potential and existing risks and typologies. Chapter 10 of the Regulation on Minimum AML/CFT Requirements requires REs to arrange regular trainings for the Board, the Executive body, the internal monitoring unit, the staff performing customer service and internal audit functions, newly recruited staff and other staff involved in the prevention of ML/FT.

An independent audit function – REs, under Article 23 of the AML/CFT Law, are required to establish rules and conditions for conducting the internal audit to check compliance with AML/CFT Law, legal statutes adopted on the basis of the AML/CFT Law, and legal statutes of the reporting entity, whenever the conduction of audit is required. According to Article 25 of the AML/CFT Law, REs are required to conduct internal audit in cases and the periodicity established by the FMC in order to ascertain adequate implementation of the obligations and functions stipulated by the AML/CFT Law. Chapter 9 of the Regulation on Minimum AML/CFT Requirements states that internal audit should be conducted according to the annual program of internal audit. Conclusions of the audit conducted should be submitted to the FMC within one week following approval by the Board of the RE (RE AML/CFT Minimum Requirements, Clause 55, 56 and 57).

In addition to that, under Article 25 (2) of the AML/CFT Law, upon the request of the CBA or reporting entities' own initiative, and in the manner established by the CBA, REs should commission external audit to check the proper implementation of the AML/CFT legislation and effectiveness of the regime. Clause 59 of the Regulation on Minimum AML/CFT Requirements specifies that CBA may request the RE to conduct an external audit in cases when the RE regularly violates the requirements of the AML/CFT legislation or engages in high-risk activities. REs are obliged to conduct external audit within one month after receiving request from the FMC and inform the FMC on conclusions of the external audit within one week upon its receipt (RE AML/CFT Minimum Requirements, Clause 60).

Chapter 9 of the Regulation on Minimum AML/CFT Requirements also requires REs having branches, subsidiaries and representations to assess compliance of their activities with the AML/CFT legislation and review the conclusions of audit conducted (RE AML/CFT Minimum Requirements, Clause 61).

Criterion 18.2 – Article 3 (1) (41) of the AML/CFT Law introduces the concept of financial group, which is defined as a "group comprising a legal person, which exercises control and co-ordinates functions over the members of the group (including the branches and (or) representations that are subject to anti-money laundering and counter terrorism policies and procedures at the group level) involved in banking, provision of investment services, central depositary or insurance (including reinsurance) and intermediary insurance (including reinsurance) services, for the application of effective consolidated supervision at the group level". REs are required, under Article 23(1) of the AML/CFT Law, to have in place and apply group-wide internal legal statutes for the prevention of ML and TF. These internal legal statutes should establish operational procedures of the internal monitoring unit; requirements on hiring, training and professional development of the staff on obligations defined by the AML/CFT legislation, potential and existing risks and typologies; rules and conditions for the conduction of internal audit. On the elements set out in the criterion:

Sharing information & group level compliance, audit and/or AML/CFT functions – with regard to policies and procedures for sharing information, Article 23 (1) (15) of the AML/CFT Law provides that financial groups are required to establish the procedures for sharing information within the group for combating ML and TF, including information on suspicious transactions or business relationships.

Confidentiality and use of information exchanged – These are governed by the confidentiality provisions under the sectorial laws (e.g. BS Law, Article (8)(2), Securities Law, Article 99).

Criterion 18.3 – The AML/CFT Law provides under Article 21 that REs are obliged to ensure that their subsidiaries, branches and representations operating in foreign countries or territories observe the measures determined under the AML/CFT legislation of the home country, if the AML/CFT legislation of the home country establishes stricter norms as compared with the laws and other legal statutes of the country or the territory, where the subsidiary, branch or representation is domiciled. In cases when the legislation of the country or territory, where the subsidiary, branch or representation is domiciled, prohibit or do not enable implementing the requirements under the AML/CFT legislation of the home country, then the subsidiary, branch or representation should undertake relevant measures to mitigate money laundering and terrorism financing risks, as well as inform the reporting entity on that matter, and the reporting entity should respectively inform the FMC.

Weighting and Conclusion

Armenia is C with R.18.

RECOMMENDATION 19 – HIGHER-RISK COUNTRIES

In its 2015 MER, Armenia was rated C with R.19. Since then, no relevant material changes have been made to Armenian legislation. Thus, the below analysis represents a summary of 2015 MER findings.

Criterion 19.1 – Article 18 (2) of the AML/CFT Law requires REs, including FIs to conduct enhanced due diligence measures in the presence of high-risk criteria, or upon an assignment made by the CBA, and when a criterion of high risk is detected or becomes apparent in the course of the transaction or business relationship. Article 3 (1) (21) of the AML/CFT Law defines the term "high-risk criterion" as a criterion indicating a high likelihood of ML or TF and include, among others, the persons (including financial institutions), which are domiciled or reside in or are from non-compliant countries or territories. Thus, whenever the reporting FIs detect that the business relationship or transactions involves natural or legal persons (including financial institutions) from non-compliant country or territory, they are obliged to apply enhanced CDD measures.

Criterion 19.2 – Armenia is able to apply countermeasures when called upon to do so by the FATF and independently of any call by the FATF to do so. REs are required to recognise customers as high risk and apply enhanced due diligence measures, which involves at minimum: a) obtaining senior management approval when the customer is found to be characterised by high-risk criteria, or when the transaction or the business relationship is found to comprise such criteria; b) taking necessary measures to establish the source of funds and wealth of the customer; c) examining, as far as possible the background and purpose of the transaction or business relationship (Articles 3 and 18 of the AML/CFT Law). In addition to that, according to Article 10 (1) (15) of the AML/CFT Law, the FMC is authorised to give assignments to REs on taking relevant measures with regard to persons (including financial institutions) which are domiciled or residing in or are from non-compliant countries or territories.

Criterion 19.3 – Armenian authorities issue a notice on the FMC website to advise REs of countermeasures or weaknesses in the AML/CFT system of other countries. This is based on data publicised by international structures active in the AML/CFT field and (or) by foreign countries. The formal letter to REs is disseminated according to the FMC internal procedures**.**

Weighting and Conclusion

Armenia is C with R.19.

RECOMMENDATION 20 – REPORTING OF SUSPICIOUS TRANSACTION

In its 2015 MER, Armenia was rated C with R.20. Since, then no material changes were introduced to the framework and thus, the below analysis represents 2015 MER findings.

Criterion 20.1 **–** The obligation for financial institutions to report suspicious transactions is found in Articles 6 and 7 of the AML/CFT Law where reporting entities are required to submit to the FMC any suspicious transactions or business relationships regardless of the amount. While dealers in precious metals and stones are only required to file an STR only with regard to cash transactions at an amount of or above AMD 5 million, this is consistent with the threshold requirements for acquiring the status of obliged entities.

The obligation applies to both the proceeds of a criminal activity and to those related to TF. FIs are also required to recognise a transaction or business relationship as suspicious, regardless of whether it matches fully or partly the criteria or typology of suspicious transactions or business relationship, which, by its nature (the logic, pattern of implementation or other characteristics), could be related to ML/TF (Part 2, Article 7 of the AML/CFT Law). There is an obligation to record and maintain the grounds for non-recognition a transaction or business relationship as suspicious, the respective conclusions and findings, as well as the process of conducted analysis in accordance with the provisions of the AML/CFT Law, in case if the suspicion of a transaction or business relationship is disproved (Part 3, Article 7 of the AML/CFT Law). The reporting of suspicious transactions related to tax crimes and other criminal activity is covered, as Armenia has an all-crimes approach to its criminalisation of ML (Article 296 of the CC).

Criterion 20.2 **–** There is an explicit requirement to report all suspicious transactions regardless of their amount. This requirement also applies to suspicious attempted transactions (Part 2 of Article 6 and Part 1 of Article 7 of the AML/CFT Law)

Weighting and Conclusion

Armenia is C with R.20.

RECOMMENDATION 21 – TIPPING-OFF AND CONFIDENTIALITY

In its 2015 MER, Armenia was rated C with R.21. Since then, changes have been incorporated in the AML/CFT Law to prescribe the information sharing possibility within a financial group. These changes are not material and thus, the below analysis represents 2015 MER findings.

Criterion 21.1 – Financial institutions and their employees (including managers) are exempted from liability when disclosing information in good faith to the FMC. Besides, the FMC or its employees are also exempted from criminal, administrative or other responsibility in case of duly performing their obligations under this Law (Part 1, Article 30 of the AML/CFT Law).

Criterion 21.2 – Reporting FIs, their employees and representatives are prohibited from "tipping off" a customer or any third party (with an exception to another member of a given financial group) about the fact that an STR or related information is being or not being filed with the FIU (Point 5 of Article 6 of the AML/CFT Law).

For FIs, the sanctions to be imposed for breaching the disclosure prohibition are covered under sector specific legislations. Sanctions for breaching the disclosure prohibition are available for DNFBPs that are legal persons are available under Point 4, Part 4, Article 30 of the AML/CFT Law. Sanctions for breaching the disclosure prohibition for DNFBPs that are natural persons (including managers of the casinos) are available under Point 4, Part 1 of Article 165.9 of the AO Code. The range of sanctions available includes warnings and fines.

Although there are no specific criminal sanctions for the violations to the AML/CFT law or other related regulations, intentional failure by individuals to comply with the AML/CFT provision could be punished under the Criminal Code, if the conduct amounts, for example, to aiding or abetting ML or TF (including attempt).

Weighting and Conclusion

Armenia is C with R. 21.

RECOMMENDATION 22 – DNFBPS: CUSTOMER DUE DILIGENCE

In its 2015 MER, Armenia was rated LC with R.22. Since R.10, R.12 and R.15 are under review, R.22 is also under review.

Criterion 22.1 – The CDD requirements for DNFBPs are the same as those applicable to FIs (AML/CFT Law, Art. 16(3)). The types of DNFBPs subject to CDD requirements include:

(a) organisers of casino, games of chance (including online) and lotteries - only when conducting transactions (single or linked occasional transactions) of at least AMD 1 million (approximately EUR 2 250). This includes purchasing of chips, accepting wagers, paying out winnings or related financial transactions.

(b) legal entities and natural persons engaged in real estate activities - only with regard to real estate purchase and sale transactions or business relationships. There is no explicit requirement to apply CDD measures to both seller and buyer of the same property. However, given the definition of customer in the AML/CFT Law, this obligation is interpreted as applying to both parties to the transaction (Art. 3(13)).

(c) dealers in precious metals and dealers in precious stones - only with regard to cash transactions at an amount of or above AMD 5 million (approximately EUR 11 000)

(d) notaries, attorneys, as well as sole practitioner lawyers and legal firms, sole practitioner accountants and accounting firms - only in relation with preparing for or carrying out the following types of transactions or business relationships: a) buying and selling of real estate; b) managing of client's funds, securities or other property; c) management of bank and securities accounts; d) provision of property for the creation, operation, or management of legal persons; e) carrying out functions involving the creation, operation, or management of legal persons, as well as the alienation (acquisition) of stocks (equity interests, shares and the like) in the statutory (equity and the like) capital of legal persons, or the alienation (acquisition) of issued stocks (equity interests, shares and the like) of legal persons at nominal or market value.

(e) Legal entities and natural persons providing services for registration or management of legal persons – only when they: a) act as a formation agent (representative) of legal persons in rendering services for registration of legal persons; b) act (arrange for another person to act) as an executive officer (member of executive body) of a company, a partner of a partnership, or perform similar functions of a legal person's management; c) provide a registered office (business address, correspondence or administrative address) to a legal person; d) act (arrange for another person to act) as a trustee or perform the equivalent function for other similar legal arrangement; e) act (arrange for another person to act) as a nominee shareholder for another legal person.

Shortcomings discussed at R.10 equally apply here.

Criterion 22.2 – Reference is made to R.11. In the particular case of trustees or managing persons of similar legal arrangements in Armenia, those have to retain identification data on beneficial owners of the trust/legal arrangement or identification data on the legal persons that are parties to the trust. (AML/CFT Law, Art. 29(3.1))

Criterion 22.3 – The PEP requirements under R.12 also apply to covered DNFBPs. The remaining minor deficiencies under c.12.4 relate to life insurance and are therefore not relevant for DNFBPs.

Criterion 22.4 **–** Reference is made to R.15.

Criterion 22.5 **–** Reference is made to R.17

Weighting and conclusion

The AML/CFT provisions applicable to DNFBPs mirror those for FIs, therefore deficiencies identified under R.10 and R.15 apply accordingly. **Armenia is LC with R.22.**

RECOMMENDATION 23 – DNFBPS: OTHER MEASURES

In its 2015 MER, Armenia was rated C with R.23. Since then, no relevant material changes have been made to Armenian legislation and thus, the below analysis represents 2015 MER findings.

Criterion 23.1 – The requirements to report suspicious transactions set out in R.20 apply to lawyers, notaries, other independent legal professionals, accountants, dealers in precious metals and stones and trust and company service providers in the circumstances referred to under c.22.1(c), (d) and (e).

Criterion 23.2, Criterion 22.3 and Criterion 22.4 – For a description of requirements on internal controls, high-risk countries and tipping-off/confidentiality reference should be made to the analysis under R.18, R.19 and R.21. The definition of TCSPs refers however, only to legal entities.

Weighting and Conclusion

Armenia is C with R.23.

RECOMMENDATION 24 – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS

In its 2015 MER, Armenia was rated LC on R.24. The remaining deficiencies related to the country's assessment of risk associated with legal persons, the lack of an explicit mechanism to ensure that basic information maintained by the State Registry was accurate and updated on a timely basis, and the lack of sanctions for failure to provide the State Registry with registration or BO information. The FATF Standards for R.24 have since been revised, and thus R.24 is being re-assessed.

A broad range of legal persons may be set up under Armenian Law. These may be commercial organisations (i.e. business partnerships – general or limited partnerships, companies - i.e. LLCs, supplementary liability companies or JSCs, and cooperatives), or non-commercial organisations (i.e. societal amalgamations, foundations/funds, unions of legal persons and other forms provided by statute such as public organisations (NGOs)). See Art. 51, 72 and 117 of the Civil Code. See Introduction to Money Laundering and Terrorist Financing Risks and Context for further information on Armenian legal persons.

Natural persons in Armenia may conduct entrepreneurial activity as sole proprietors/entrepreneurs which does not entail the creation of a separate legal person and hence are not considered legal persons for the purposes of this analysis.

Criterion 24.1 – The requirements of R.24 are applicable to legal persons as follows: (a) Companies (i.e. LLCs and JSCs) are subject to the requirements of R.24 as set out in this analysis; (b) Business Partnerships (i.e. GPs and LPs) and Foundations – are subject to the requirements of R.24 as set out in this analysis; (c) Other types of legal persons – As set out in the introduction, NGOs and Cooperatives are considered to be other relevant (in terms of materiality and risk) types of legal persons. These are subject to the basic information requirements set out in this analysis; (d) Foreign created legal persons – Foreign legal persons with sufficient links to Armenia were subject to a ML/TF risk assessment, although deficiencies have been noted (c.24.3(b)). Moreover, the mechanisms (and combination thereof) to ensure availability of BO information for foreign legal persons are not deemed sufficient (see c.24.10).

Criterion 24.2 –

(a) The types, forms and basic features of legal persons that may be established under Armenian Law are set out under Chapter 5 of the Civil Code, and separate laws providing further detail in respect to specific types of legal persons (i.e. Law on LLCs – LLCs, Law on JSCs (covering OJSCs and CJSCs), Law on Foundations, Law on Condominium, Law on Trade Unions, Law on Consumer Cooperatives, Law on Agricultural Cooperatives, Constitutional Law on Parties, Law on Freedom of Conscience and Religious Organisations, Law on Employers' Union, and Law on Chamber of Commerce and Industry). These laws are publicly available, including online through the official websites of the National Assembly[103] and the Government[104].

(b) The Civil Code, the LP Registration Law and the above-mentioned specific laws provide information on the processes for the creation of the different types of legal persons. Basic information on the process of registration, samples of documents required for registration, relevant laws and rules in Armenian language may also be found at the State Registry website[105].

(c) The process for recording of basic and BO information is set out in the LP Registration Law (see Art. 8, 32-36, 37-39, 42, 60.1-60.4). The process for the obtainment of basic and BO information is set out under Art. 61-66 of the same law.

Criterion 24.3 –

(a) ML/TF risks of legal persons are analysed in the NRA 2021 and NRA 2024 (the latter includes a brief section for legal arrangements). In addition, a separate more elaborate ML/TF risk assessment was carried out for the legal persons. The findings are analysed at large in IO.5 together with the deficiencies in the comprehensiveness of the analysis which impacts the rating for this criterion.

Following the NRA 2024, there are limited action points in the 2025-2028 National AML/CFT/CPF Strategy (e.g., consider adding BO data onto the register on bank accounts as well as consider

[103] National Assembly of the Republic of Armenia | Official Web Site | parliament.am

[104] https://www.arlis.am/en/

[105] https://e-register.moj.am/en/

introducing procedures for reporting inconsistencies regarding BO data). The adoption of the Anti-Corruption Strategy 2023–2026 predates both the NRA 2024 and the National AML/CFT/CPF Strategy 2025–2028. It remains unclear whether the vulnerabilities identified in the NRA 2024, particularly those related to legal persons, are being mitigated and /or any mitigating actions have been completed to date. The 2023-2026 Anti-Corruption strategy does include measures to ensure interoperability of various BO registers and the issuance of BO-related guidelines. On 10 June 2025, the Agency was interconnected with the Government Interoperability Platform, specifically integrated with the web services of the Corruption Prevention Commission, to ensure access to relevant information on beneficial ownership. Interoperability with the shareholders' register is not yet established. Although these measures are commendable, it is important to note that, during the assessment period, Armenia had not implemented sufficient mitigating measures to ensure that competent authorities have timely access to adequate, accurate, and up-to-date BO information for legal persons.

(b) Armenia assessed the risks of foreign legal persons in the legal persons' risk assessment covering the period 2021-2023. Armenia informs that a sufficient link to the country when assessing foreign legal persons was considered, which takes the form of business activities, business relationship with reporting entities, physical establishment (including through branches and agencies), presence of real estate investments, country of origin of BOs, the existence of BOs (or similar functions) of Armenian nationality. There are some gaps that affect the completeness of the analysis: i) subsequent changes in ownership of foreign legal persons that attain permanent establishment status in Armenia are not available to the SRC; and ii) there is no dedicated register of BO data for foreign legal persons, and not all such legal persons have a bank account in Armenia, limiting access to BO information (see IO.5). Consequently, mitigating measures are not fully in place which impacts the rating attributed to this criterion.

Criterion 24.4 **–** Art. 56 of the Civil Code stipulates that legal persons are subject to state registration and are deemed created at the moment they are registered.

In accordance with Art. 12 of the LP Registration Law, the Agency is responsible for conducting the registration of legal persons, maintain the State Registry of legal persons and publishing or providing information held in the State Registry.

Article 22(1) and 26 of the LP Registration Law set out the documentation and information that must be recorded in the State Registry for legal persons. This includes most of the basic information set out under c.24.5(a) (including the charter of the legal person containing the basic regulating powers which must be registered – see Art. 34(1)(3)). There is no requirement to register and record the list of all the directors, but only the details of the head of the executive body.

Article 6 of the LP Registration Law states that all registered information is publicly available except for certain personal data. Most of the basic information set out under c.24.5(a) is publicly available in the following manner:

- through the website of the Agency free of charge (i.e. the name, legal form, taxpayer identification number, place of location (i.e. registered office – see Art. 59 of the Civil Code) and status (i.e. information on whether the legal person is in the process of liquidation or removal from record-registration). See Art. 61(2) of the LP Registration Law.
- upon the request of any person, through the website and or in paper form, and subject to the payment of a fee (i.e. copies of the charters of legal persons which include their basic regulating powers). See Art. 61(3) and (5) – LP Registration Law.
- through the obtainment of a uniform excerpt which confirms state registration and which amongst other basic information should also include the name and head of the executive body of a legal person or another person entitled to represent the legal person. There is however no requirement to make public, information on all directors. See Art. 62 – LP Registration Law.

Criterion 24.5 –

(a) **Basic Information -** There is no explicit obligation for legal persons to obtain and record basic information. For most legal persons there are indirect obligations to retain some of the basic information as follows:

LLCs and JSCs – Are required to draw up and register a charter which must include the (name of the legal person indicative of the form, its place of location and basic regulating powers – see Art. 55 and 95(2) of the Civil Code and Art. 10(2) of the LLC Law). The LLC is obliged to give access to auditors and shareholders to the charter which thus indirectly obliges the LLC to retain the charter and amendments thereto for this purpose – see Art. 10(3) of the LLC Law. Similar provisions are applicable to JSCs (Art 4(1), 14(1), (2) and (3) of the JSC Law, and Art. 55 of the Civil Code).

Foundations – Similar provisions are applicable to Foundations (see Art 5(1), 15 and 20(2) of the Law on Foundations and Art. 55 of the Civil Code).

NGOs – NGOs are required to draw up a charter/articles of association which set out the name indicative of the legal form, registered office, list of members of the executive body, and the basic regulating powers. NGOs are bound to allow their members to inspect the articles of association upon request and are thus indirectly obliged to retain the articles of association. See Art. 6(2), 13 and 18(5) of the Law on Public Organisations and Art. 55 of the Civil Code.

For partnerships and cooperatives there are no direct or indirect provisions requiring them to retain the charter inclusive of the basic information set out under c.24.5(a).

All legal persons are in terms of the LP Registration Law required to submit to the registry most of the basic information set out under c.24.5(a), for the legal person to be established (i.e. name indicative of legal form, registered office, basic regulating powers and details of the head of the executive body- see Art. 32, 32.1, 34(1)(3) and 34(1)(5) of the LP Registration Law. Legal persons are not required to register a list of all directors. Article 55(3) of the Civil Code moreover states that changes to the charter (including the most relevant basic information) only takes effect upon registration. This has the effect of mandating the registration of changes.

Thus, while most basic information set out under c.24.5(a) is subject to registration (see c.24.4), not all legal persons are required to obtain and record this information. Moreover, while indeed most material legal persons are required to keep some basic information this excludes proof of incorporation, status and information on directors.

(b) **Register of Shareholders/Members** – LLCs are required (indirectly – see para (a)) to retain the charter of the legal person which ought to include the name and other identification information of the company participants and the size of their shares (LLC Law, Art 10). In the case of LLCs there are no different types of shares or voting rights, the volume of shares held is equivalent to the contribution of each shareholder to the total capital of the LLC (LLC Law, Art. 27, 28(3) and 35(1)). As set out under para (a) LLCs are bound to give access to the charter and amendments thereto, which thus indirectly necessitates the retention of amendments to the charter.

JSCs – A register of shareholders is to be maintained by the Central Depository, including information on the amount, type and class of securities registered in shareholders' names (Law on Joint Stock Companies, Art. 51; Securities Law, Art. 176 (1)(2)). Article 32 of the Law on JSCs stipulates that upon allocation of shares the JSC must register the shares of the shareholders in their personal accounts, while shareholders and nominees are obliged to inform the Central Depository of any shareholding changes (Art 32(4) of the Law on JSCs)

Foundations – The charter of a foundation must include information on the founders (name, surname, place of residence, registered office and country of registration) – Art. 15(2) and (2.1). Foundations do not have ownership interests organised in shares, but rather founders and donors who contribute to the cause of the foundation or to the benefit of the beneficiaries of the foundation (see Art. 3 of the Law on Foundations). In accordance with Art. 20(2) foundations must indirectly keep a record of the charter and amendments thereto.

NGOs – In accordance with Art 18(1) of the Law on Public Organisations NGOs must maintain a register of members (i.e. any person joining the organisation after registration – Art. 5(1)) and volunteers.

Partnership and Cooperatives - There are no requirements for partnerships and cooperatives to retain information on their partners and or members including names and types of partners and the value of their contribution to the partnership's capital.

Considering that the most material legal persons are bound to keep information on shareholders and/or members, this sub-criterion is deemed to be mostly met.

(c) **Location of Records –** There is no requirement for legal persons, nor the Central Depositary in the case of JSCs to keep the register and information on shareholders or members within the country. However, the State Registry holds BO information in Armenia (see c.24.6(b)(i)) and legal persons are required to provide competent authorities, including LEAs and FIU, with the BO information requested (see c.24.9).

***Criterion 24.6* -** The definition of BO for legal persons is set out under Article 60.1 of the LP Registration Law by cross-reference to the definition under the AML/CFT Law (see analysis under c.10.10) and is largely in line with the FATF Standards.

Armenia adopts a multi-pronged approach to ensure that BO information on legal persons is available in a timely manner, by requiring legal persons themselves to keep such information, requiring BO information to be registered with the State Registry, and through FIs and DNFBPs undertaking CDD on clients that are Armenian legal persons. The current BO registry was established and expanded as part of anti-corruption strategies (2019-2022 and 2023-2026 Anti-Corruption Strategies) and legislative amendments, with significant platform improvements launched in December 2025, including interconnection with government databases. Although documented steps show progressive development, authorities did not provide a single decision outlining the choice of most appropriate mechanism based on national risks, context and materiality.

(a) Legal persons are required to possess reliable information on their actual beneficiaries and on the grounds of being an actual beneficiary (Art. 60.2(1), LP Registration Law). While not expressly defined, the term reliable is interpreted to mean, information that is adequate, accurate and up-to-date. This since Art. 60.2 stipulates that in order to disclose reliable information, legal persons must conduct periodical (at least every year) due diligence on beneficial ownership, including following up and enquiring when there are doubts. Moreover, in accordance with Art. 60.3(2) legal persons must provide a declaration on the actual beneficiaries, including identification details of such beneficiaries, to the State Registry upon registration and subsequent to any changes. Thus, they must obtain identification details set out in the law which are considered adequate to lead to the identification of the individual beneficiaries.

Information regarding BOs and the conducted periodical reviews must be made available to the requesting competent authority within five days (LP Registration Law, Art. 60.2(2)). LEAs have access to the beneficiary information stored in the State Registry (see c.24.9).

Legal persons are not explicitly required to co-operate with FIs/DNFBPs to provide accurate, adequate and up-to-date information on BOs. This is somewhat mitigated by the fact that FIs/DNFBPs are prohibited from executing transactions and establishing or continuing business relationships where CDD (including BO information) is not provided (see c.10.19).

(b) (i) Legal persons are required to submit their BO declarations, including reliable BO identification information and information on the grounds based on which a person is a BO, to the State Registry (LP Registration Law, Art. 60.3(1), (2)(5), 2(6) and (4)). This must be provided within 40 days of the registration of the legal person or of becoming aware of changes to BO information.

The State Registry is required to keep records of BO information (see Art. 26(1)(24)) and maintain persistent supervision to ensure the reliability of BO information (Art. 60.5(1) of the LP Registration Law). The online platform for submitting BO declarations also has features aimed at ensuring the accuracy of submitted information via the use of required fields, formatted fields, auto-filled fields, and cross-checks between linked fields. As set out above any changes to BO information must be registered within 40 days, while on a yearly basis (20th February of each year) the legal person must submit to the Agency a confirmation that BO data is up to data or declare any changes thereto. These provisions are subject to enforcement actions (see c.24.14).

(ii) No alternative mechanism to the BO Register is envisaged.

(iii) BO information is also available via FIs/DNFBPs which are obliged when establishing a business relationship or carrying out an occasional transaction with a legal person to carry out CDD, maintain CDD information up-to-date and keep CDD records (see analysis under c.10.10, c.10.7(b), R.11, c.22.1 and c.22.2). Minor shortcomings identified under c.10.10 and c.22.1 impact compliance with this criterion.

Criterion 24.7 – All legal persons in Armenia are required to maintain BO information for at least five years after a person ceases to be a BO of the legal person (LP Registration Law, Art. 60.2(2)). This is not fully in line with the standards which require BO information to be kept for at least five years after the legal person ceases to exist. No information was provided on any legal provisions requiring administrators, liquidators or other persons involved in the dissolution of the company to keep records after the legal person is dissolved or cease to exist.

The State Registry maintains all information held in the Registry (including BO information) on liquidated legal persons permanently. The archive file (including paper documentation) shall be retained for 10 years after a legal person terminates its activities and is subject to destruction thereafter (LP Registration Law, Art. 22(2)).

FIs and DNFBPs are required to keep CDD (including BO information) for five years from the termination of the business relationship or the completion of the transaction with a customer (see c.11.1 and c.22.2).

Criterion 24.8 – **Basic Information** – As set out under c.24.5 some legal persons are required to retain some basic information, while most material legal persons are bound to keep information on shareholders and/or members (within the Charter – LLCs and Foundations, or in a separate register – NGOs). As set out under c.24.4 basic information (except the list of all directors) is subject to registration at the State Registry as is the information on shareholders/members (LP Registration Law, Art. 26(1)(10)(11)). Given that only registered information is valid and legally enforceable, all basic information held by the State Registry is considered accurate and up-to-date.

There are some further mechanisms to ensure that basic information is adequate, accurate and up-to-date:

- Changes in persons details of Armenian citizens involved in Armenian legal persons (e.g. as participators or directors) within the Government database are automatically updated in the State Registry (Art. 37 of the LP Registration Law); and
- Changes to the charters of legal persons (including some basic information, and shareholder information in case of LLCs and Foundations) only take effect upon registration (Art. 55(3) –

Civil Code). While for JSCs the onus is on the shareholders or nominees to register shareholding and Art 51(4) of the JSC Law stipulates that neither the JSC nor the Central Depository is liable for any damages resulting from failure to register. In the case of JSCs, any change in ownership rights becomes effective only upon registration in the name of the buyer (or their nominee) with the Central Depository or another custodian.

Beneficial Ownership Information – As explained under c.24.6(a) legal persons are bound to keep reliable BO information. In the case of foreign BOs authenticated copies of identification documents are required for registration (LP Registration Law, Art. 60.4(3)).

To ensure that BO information is up-to-date the LP Registration Law obliges beneficiaries to inform the legal person within 20 days of becoming a beneficiary (Art. 60.2(4)), while legal persons themselves are bound to register such changes in BO information within 40 days of become aware of a change (Art. 60.3(4)), which could extend the registration of updated BO data for up to 60 days. Legal persons are moreover bound to submit an annual confirmation of registered BO data (see c.24.6(a)).

In addition, the Agency is empowered to maintain persistent supervision to ensure the reliability of BO information (Art. 60.5 of the LP Registration Law) and the online platform for the registration of BO data has inbuilt data accuracy checks. Furthermore, state bodies that identify any discrepancies in BO data are required to notify the Agency (Art. 60.5(2)).

Enforcement actions and sanctions are also envisaged for the non-submission of BO information as required, or for the negligent or wilful submission of wrong or incomplete data (see c.24.14).

FIs/DNFBPs are subject to CDD and record keeping obligations that require them to identify and verify the identity of BOs of clients that are legal persons, and to keep such information up-to-date. They are subject to AML/CFT supervision and sanctions to ensure compliance with these obligations (see c.24.6, R.26, R.28 and R.35). However, there is no legal requirement for a legal person to have a business relationship with FIs/DNFBPs.

Considering the lengthy timeframe for registering BO changes and the absence of a legal requirement for legal persons to maintain a business relationship with FI/DNFBP, these mechanisms are not deemed sufficient to ensure that available BO information is adequate, accurate and up-to-date.

***Criterion 24.9* - Access to the basic and BO information held in the State Registry and Central Depository**: Complete information stored in the State Registry (which includes basic and BO information for all legal persons, as well as shareholders' information for all legal persons other than JSCs) must be provided (via login credentials) to state bodies online through the Agency's website (see Art. 65). The authorities explained that such access has been granted to various state bodies including LEAs, prosecutors, supervisory authorities, tax and customs authorities and the FMC. Some basic and BO information is also publicly available through the online website of the Agency (see Art. 61(2)(7) of the LP Registration Law).

In the case of JSCs information on nominal shareholders and shareholding details, as well as information on the owners of stocks held under nominee and retained or obtainable by the Central Depository is directly accessible to prosecutors, LEAs, the national security service and tax and customs authorities (Securities Law, Art. 98(2)(6), and 98(3)). Access to this information is provided either via direct access to the electronic data information system, or upon request in the case of data on the owners of stock under nominee which is not held at the Central Depository but obtainable upon request (Securities Law, Art. 197(13)). The submission of data on the owners of stock upon request must be provided within 9 working days (Securities Law, Art. 197(2), (3), and (9)), which is not deemed to ensure timely access.

Access to the basic and BO information held by legal persons: State bodies have access upon request to documentation on BOs held by the legal persons when this is required for the purpose of implementing their powers. Such documents should be made available immediately and not later than five days (LP Registration Law, Art. 60.2(2)). The term "state bodies" is not defined and hence not clear whether this covers all competent authorities.

As set out under c.24.5 there are moderate and minor gaps in the basic and shareholder information available at legal persons, which impact the usability of legal persons as a source to obtain such information.

Access to the basic and BO information held by FIs and DNFBPs: Prosecutors and LEAs can obtain information held by FIs/DNFBPs (including basic and BO information obtained through the application of CDD), however as set out under c.31.1(a) this is limited, and requests may be refused when they concern attorney information or banking or related secrecy. Prosecutors and LEAs may obtain such information indirectly, by requesting the FMC if there is a justified suspicion of ML/TF (AML/CFT Law, Art. 13(4)). The FMC would however be able to supply such information only if it is available to it, and within a maximum of 30-days, which is also not considered timely.

The FMC, the CBA and MoJ have access to all and any information held by FIs/DNFBPs (see c.27.3, c.28.4(a), and c.29.3). Some DNFBP supervisors (i.e. the SRC and the ChoA) have limitations in their ability to obtain information from supervised entities (see R.28).

Access to information in the course of public procurements: When applying to participate in public procurement processes, legal persons are required to submit either a reference to the page of the State Registry website with their published BO information or, in case of foreign legal persons, to fill-in and submit the same BO declaration form used for the State Registry (Law on Procurement, Art. 28(2)(2)(b)).

Criterion 24.10 - Information on BO of foreign legal persons with sufficient links to Armenia may be obtained from (i) FIs and DNFBPs as described in c.24.9, if a foreign legal person has a business relationship with a RE, and (ii) from public administration bodies (contracting authorities) managing public procurement processes when foreign legal persons participate in such processes.

Given that there are no legal requirements for foreign legal persons to open business relationships with Armenian REs when doing business in Armenia and considering that the availability of BO information through public procurement processes would only cover those participating foreign legal persons, these mechanisms are not deemed sufficient.

***Criterion 24.11* – Access to Registered Data for FIs/DNFBPs** - As set out in c.24.4 some registered information held in the State Registry is accessible to the public free of charge (hence including FIs and DNFBPs) on the Agency's website.[106] More complete information and documentation (including copies of charters) is available via the online website or in paper form subject to a fee. Furthermore, Art. 65(2) requires the Agency to provide notaries, banks and advocates with login credentials to gain access to the Registry and retrieve data automatically.

Access to Registered Data for foreign competent authorities – As set out above some information held in the State Registry is accessible to the public free of charge (hence including to foreign competent authorities). This would include a comprehensive set of details covering most of the basic information set out under c.24.5(a) except for the basic regulating powers (available publicly for a fee) and the list of directors. The latter may only be obtained via the formal and informal international cooperation channels.

Criterion 24.12 - (a) It is prohibited to open, issue, provide and service bearer securities (AML/CFT

[106] Available at https://e-register.moj.am/en/.

Law, Art. 15(1)(3) and Art. 7 of the Securities Law).

(b) Since the adoption of the first Law on JSCs in 1996, company shares were required to be registered in the name of the nominal or actual holder (Art. 54), and hence no JSC bearer shares ever existed. The AT was not informed whether in the case of LLCs, the law has required from the adoption that the ownership interests/parts were required to be registered and could not be transferred anonymously (as bearer instruments). The authorities however explained that to their knowledge there were no LLC bearer shares in circulation and if theoretically there were, the attached rights are no longer exercisable as according to Art. 332 of the Civil Code civil actions are time barred after three years, and the requirement for LLC shares to be registered existed for more than three years.

Criterion 24.13 – (a) The concept of nominee shareholder is expressly mentioned and regulated in the context of JSCs under the Securities Law. There are no explicit legal provisions requiring nominee shareholders or directors to disclose their status or the identity of their nominator to the company or the relevant register.

(b) Article 194(4) stipulates that nominee securities account at the Central Depository may only be held by custodians (regulated by the CBA – see Art. 193) or foreign persons entitled by the laws of their country to hold shares as nominees. Point 258 of the Central Depositary Rules on Operating Unified System of Securities Registration and Settlement stipulates that those opening nominee securities accounts (both Armenian and foreign custodians) must present a copy of the permit/license to carry out custody service to the Central Depositary.

Point 116 of the above-mentioned rules states that the Central Depositary must maintain in the register of securities information on nominee owners, while custodians must distinguish the nominee account by a special note (Art. 194(4) of the Securities Law). The Central Depositary is not required to maintain information about the nominator and, where applicable, the BOs, on whose behalf the custodian is acting. However, upon request custodians (domestic and foreign) must be able to provide this information to the Central Depositary which may also act on behalf of a request by competent authorities (see Art. 197(7) and (13) and point 80.1 of the Central Depositary Rules).

(c) There is no explicit prohibition of the use of nominee shareholders or directors. In the case of LLCs, these are neither expressly permitted nor prohibited from allowing nominee participants/shareholders and/or directors; therefore, the measures outline under points (a) and (b) of this criterion are not applicable.

Criterion 24.14 - **Sanctions for legal persons**: *Administrative Sanctions -* As set out under c.24.5 some legal persons are required to retain some basic information and information on shareholders/members. Moreover (as set out under c.24.4) most basic information is subject to registration at the State Registry as is the information on shareholders/members for legal persons other than JSCs (see Art. 26(1)(10)(11). In the case of JSCs shareholder information is registered and maintained by the Central Depositary. Basic and shareholder information and changes thereto, take effect only upon registration. Other than this, no information was provided on any sanctions available to enforce the obligations to obtain and keep adequate, accurate and up-to-date basic and shareholder information.

In the case of BO information breaches there are a series of administrative sanctions envisaged under Art. 169.29 of the AO Code for legal persons. Failure to submit information on the actual beneficiaries to the Registry, submission of incorrect or incomplete BO information due to negligence, and failure to conduct periodical due diligence on the beneficiaries and retain records are subject to a warning or the imposition of an administrative fine in the amount of thirty to one hundred times the established minimum wage (approximately EUR 16 800 - i.e. ten times the minimum monthly wage of AMD 75 000 equivalent to EUR 168 as at January 2026).

Art. 169.29 goes on to say that the legal person shall be released from administrative liability where before the imposition of the administrative fine it eliminates the violation committed. Furthermore Art. 37(3) of the AO Code stipulates that the administrative action must be initiated within two months from when the breach is discovered, which might impact the conduct of proper analysis of breaches and of successful proceedings.

Additionally, in case of failures to submit annual BO declarations for three consecutive years, or in the case of multiple or gross violations of the BO information obligations, the Agency may apply to court to have the legal person liquidated (LP Registration Law Art. 60.5(6)).

Criminal Sanctions – The provision of false BO data or the concealment of BO information is punishable by a fine in the maximum amount of ten-fold of the monthly income of the perpetrator (if the perpetrator's income is unavailable, undetermined, or below the minimum monthly salary, the fine is based on the minimum monthly salary at the time of the offence), or deprivation of the right to hold certain positions or exercise certain activities for a term of maximum three years, or imprisonment for a maximum term of three years (Art. 294 and 59 of the CC). Article 125 of the CC however stipulates that a legal person shall be released from criminal liability if it eliminates the causes and conditions contributing to the commission of a criminal offence.

The administrative, criminal and forced liquidation sanctions taken together are considered to constitute effective and dissuasive sanctions for BO information breaches, and moreover the law provides ranges to ensure proportionality. Nonetheless the provisions of the AO Code and CC Code extinguishing administrative and criminal liability when a breach is remedied and the restrictive time limitations to institute administrative proceedings significantly hamper the effectiveness of these sanctions, especially in so far as serious, systemic and repeated breaches are concerned. Furthermore, no information was provided on sanctions applicable to legal persons or their representatives for failure to provide basic or BO information to competent authorities upon request.

Sanctions for FIs/DNFBPs: FIs and DNFBPs are subject to administrative sanctions for non-compliance with CDD requirements (including the obtainment and recording of basic and BO information on corporate clients). In the case of FIs these sanctions are deemed effective, dissuasive and proportionate. This is however not the case for DNFBPs (see R.35).

No information was provided on sanctions envisaged for FIs/DNFBPs for failure to provide information upon request to the competent authorities.

Criterion 24.15 – (a) As set out under c.37.3 and c.37.4 there are no unreasonable or unduly restrictions applicable for the provision of international MLA except for some minor technical deficiencies. However, in the case of informal international cooperation the AT did not have enough information to be able to determine whether the laws or procedures impose unreasonable or unduly restrictive conditions (see c.40.5).

(b) and (c) The basic and shareholder information set out under c.24.5 and held in the Register is directly accessible to foreign competent authorities, in some cases for a fee (see c.24.11). However, in case of JSCs, shareholder information can be obtained through formal and information cooperation channels via counterpart authorities which may use their domestic access powers also to assist foreign counterparts (see c.37.8 and c.40.8).

(d) Armenian competent authorities may use their domestic powers to obtain evidence and information to assist foreign counterparts (thus including BO information). See analysis under c.37.8 and c.40.8.

(e) No information was provided on the existence of a dedicated mechanism to monitor the quality of assistance for basic and BO information received.

(f) As set out under c.24.9 BO information is required to be registered in the State Registry, and the Agency is responsible for keeping and making accessible such information.

(g) The authorities responsible for responding to MLAs and other forms of international cooperation are set out in the respective laws which are publicly available (see c.37.1 and c.40.2(a)).

Weighting and Conclusion

While the majority of criteria under this Recommendation are met or mostly met, there are several critical criteria that are only partly met (c.24.3, c.24.8, c.24.9, c.24.10, c.24.13 and c.24.14). The AT placed more weight on the following when reaching a conclusion on the level of compliance achieved for R.24: (i) There are insufficient mitigating measures implemented to ensure timely access to adequate, accurate and up-to-date BO information, both for legal persons registered in Armenia and for foreign legal persons with sufficient links to Armenia (c.24.3); (ii) There are certain circumstances when LEAs are not empowered to source basic and BO information from FIs and DNFBPs, and the gaps in basic and shareholder information held by legal persons also impact the relevance of legal persons as a source; (iii) The sanctioning regime for basic and BO information breaches by legal persons are not deemed effective and dissuasive in view of the extinguishment of liability when breaches are remedied (even when these are serious, systemic, or repetitive breaches), and the statute time limitation to institute proceedings (c.24.14). Other relevant deficiencies underpinning criterion assessed as partially met included: (i) Not all legal persons are required to obtain and record the basic information set out under c.24.5(a), and while most material legal persons are, this excludes proof of incorporation, status and information on directors – c.24.5(a); (ii) The absence of requirement for legal persons and the Central Depositary to keep shareholder information in Armenia – see c.24.5(c); (iii) Partnerships and cooperatives are not required to retain information on their partners or members – see c.24.5(b). (iv) Data on the owners of stock of JSCs must be provided to competent authorities within nine working days which is not deemed timely – see c.24.9. (v) The combination of mechanisms to ensure the availability of BO information for foreign legal persons are not sufficient – see c.24.10. (vi) In the case of LLCs, no measures to prevent or mitigate the misuse of nominees are in place – see c.24.13. **R.24 is rated as PC.**

RECOMMENDATION 25 – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS

In its 2015 MER, Armenia was rated LC with R.25. LEAs had restricted powers to obtain information held by FIs and DNFBPs on the BO and control of the trust. The FATF Standards for R.25 have undergone a revision against which the country has not previously been assessed. On this basis, R.25 is regarded as a recommendation under review.

Criterion 25.1 – Armenian law does not permit the formation of express trusts or other legal arrangements, and Armenia is not signatory to the Hague Convention. There is nothing in Armenian law precluding foreign trustees to operate in Armenia and/or contract a business relationship with an FI or DNFBP in Armenia. Article 3 of the AML/CFT Law provides that entities providing trust management services are reporting entities, and as such are required to conduct CDD and obtain BO information as detailed in Article 3(14).

Criterion 25.2 – Armenian law does not recognise trusts or other similar legal arrangements.

Criterion 25.3 – (a) There are no trusts governed under the Armenian law;

(b) and (c) The 2024 NRA does not include a dedicated section assessing the ML/TF vulnerabilities of legal arrangements. Legal arrangements are referenced briefly in the separate ML/TF risk assessment of legal persons. The assessment of risks of abuse for ML/TF through legal arrangements drew on inputs from reporting entities, exchanges with foreign FIUs, information from law enforcement and supervisory authorities, and the State Registry Agency, concluding that that the ML/TF risk associated with legal arrangements is low, given the absence of foreign trusts operating in Armenia, the absence of trustees/trust managers in the customer base of reporting entities during 2021-2023; and the lack of international co-operation requests or STRs involving legal arrangements. However, there is no structured analysis on the ML and TF vulnerabilities in relation to legal arrangements, nor an assessment of the effectiveness of controls. In particular, the ML/TF vulnerabilities and mitigating measures related to foreign trusts and similar legal arrangements with sufficient links to Armenia have not been analysed.

Criterion 25.4 –The trustee or managing person of other similar legal arrangement (which covers persons holding equivalent position in a similar legal arrangement) that resides in or manages property located in Armenia is required to retain the following information: (a) identification data of BOs of the trust or other similar legal arrangement; which include the settlor(s), the trustee(s), the protectors (if any); each beneficiary(ies) or, where applicable, the class of beneficiaries and objects of a power and any other natural person(s) exercising ultimate effective control over the trust; (b) when the parties to the trust or other similar legal arrangement are legal entities or legal arrangements – information on their BO; and (c) identification data of persons acting on behalf of the trust or other similar legal arrangement or rendering services thereto (AML/CFT Law, Art. 29(3.1)).

Criterion 25.5 – The trustee or managing person of other similar legal arrangement that resides in Armenia or manages property located in Armenia shall be obliged to retain information detailed in c.25.4 for at least five years after the business relationship is ended, or after the date of the transaction (AML/CFT Law, Art. 22(2)).

Criterion 25.6 – There is no requirement for information discussed at c.25.4 to be kept accurate, up-to-date and to be updated within a reasonable period following any change.

Criterion 25.7 –

(a) When conducting an occasional transaction above threshold or establishing a business relationship with the reporting entity, the customer that is a trustee or managing person of other similar legal arrangement shall be obliged to reveal its status (AML/CFT Law, Art 16(7.1)).

(b) The competent authorities, including LEAs, have powers to compel information from trustees and persons managing similar legal arrangements (AML/CFT Law, Art. 29(4)). The FMC can also request information held by the reporting entities based on Article 10(1)(4) of the AML/CFT Law. No information was provided on whether requests for BO information by AML/CFT supervisors must be complied with in a timely manner.

(c) There is no prohibition set out in the laws or enforceable means for the trustees (or persons holding similar positions) to provide FIs or DNFBPS, upon request, with information regarding beneficial ownership. Reporting entities may not conduct transactions or establish business relationships unless CDD information is provided (see c.10.19). Information on trust assets that would be held or managed under the respective business relationship would also be covered under CDD i.e., information to understand the customer's business profile and source of funds of specific transactions (see c.10.6 and c.10.7(a)).

Criterion 25.8 – Trustees and persons managing similar legal arrangements are required to collect identifying information of natural person BOs, of legal persons BOs where trustee or any other party to the legal arrangement is a legal person, and of persons acting on behalf of trust or other similar legal arrangement or rendering services thereto. There is no explicit legal requirement for trustees and persons managing similar legal arrangements to ensure accuracy and that information kept is up to date.

Reporting entities conducting transactions or establishing business relationships with trustees are subject to CDD, risk-based ongoing monitoring and record keeping requirements (see analysis under c.24.6), which ensures that information held on trusts by reporting entities is required to be adequate, accurate and up-to-date (AML/CFT Law, Art. 16). There are also sanctions envisaged for breaches of AML/CFT obligations.

Criterion 25.9 – FIs and DNFBPs can be used as a source of basic and BO information on trusts and other similar legal arrangements, and this information is accessible to all competent authorities. There is no explicit legal requirement to identify trust assets. However, reporting entities are required to obtain and hold CDD information on customers who are trusts or foreign legal arrangements when conducting CDD. This includes basic and BO information, and information on trust assets if necessary for CDD purposes (see c.25.7(c)).

Criterion 25.10 – The FMC has powers to compel information from reporting entities based on Article 10(1)(4) of the AML/CFT Law. The Law does not explicitly prescribe to hold information on residence of trustees and assets held or managed by the reporting entity, but this information is collected in the scope of CDD measures (AML/CFT Law, Art. 16(4)). Powers to obtain timely access to information held by trustees or persons holding equivalent positions is in line with Art. 29(4) of AML/CFT Law. The information does not cover information on the trust assets that would be held or managed under the respective business relationship.

Criterion 25.11 – (a) and (b) TCSPs are reporting entities and thus, sanctions for AML/CFT breaches discussed at R.35 are applicable to them. Sanctions for reporting entities are provided in Art. 30(4) of AML/CFT Law, with the possibility of a fine from EUR 1 100 – EUR 11 000. In addition, a legal person trustee or a managing legal person of other similar legal arrangement are subject to a warning or imposition of a fine for breaches of the requirements in c.25.4. Sanctions for trustees are provided in Art. 30(4.2) of AML/CFT Law, with the possibility of a fine from EUR 230 to EUR 2 300. For trustees or persons holding equivalent positions that are natural persons sanctions are defined in Article 165.9 of the Administrative Offences Code, however these sanctions do not address failures to perform the obligations defined in Article 29 of AML/CFT Law which covers the requirements of c.25.4. (c) No information available on sanctions for failing to grant to competent authorities' timely access to information referred to in c.25.4 and 25.5 held by trustee or person holding equivalent position.

Criterion 25.12 – (a) As set out under c.37.3 and c.37.4 there are no unreasonable or unduly restrictions applicable for the provision of international MLAs except for some minor technical deficiencies. However, in the case of informal international cooperation the AT did not have enough information to be able to determine whether the laws or procedures impose unreasonable or unduly restrictive conditions. (b) There is no authority or registry holding information on foreign trusts or similar legal arrangements in Armenia. (c) LEAs, FIU and AML/CFT supervisors have the necessary powers to compel the production of trust information from FIs/DNFBPs (see c.25.7(b)). This information can be obtained through formal and information cooperation channels via counterpart authorities which may use their domestic access powers also to assist foreign counterparts (see c.37.8 and c.40.8). (d) Armenian competent authorities may use their domestic powers to obtain evidence and information to assist foreign counterparts (thus including BO information). See analysis under c.37.8 and c.40.8. (e) The authorities responsible for responding to MLAs and other forms of international cooperation are set out in the respective laws which are publicly available (see c.37.1 and c.40.2(a)).

Weighting and Conclusion

In Armenia trusts cannot be established, however, there is nothing in the law precluding foreign trustees to operate in Armenia and/or contract a business relationship with an FI or DNFBP in Armenia. Notwithstanding the risk assessment's conclusion that country's exposure to foreign legal arrangements is limited and no trustee clients were serviced by reporting entities between 2021 to 2023, the ML/TF vulnerabilities of legal arrangements and the effectiveness of mitigating measures were not assessed. Overall, the framework to ensure transparency of BO of legal arrangements has improved with legislative amendments in force since August 2025, but significant deficiencies remain, particularly regarding BO verification measures. Trustees and persons managing similar legal arrangements are not obliged to verify the identity of the BOs of trust parties that are legal entities or arrangements. There is no requirement that the BO information is kept accurate and up-to-date by the trustees and persons managing similar legal arrangements. **Armenia is PC with R.25.**

RECOMMENDATION 26 – REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

In its 2015 MER, Armenia was rated LC with R.26, based on the following shortcomings: several deficiencies in the application of measures to prevent criminals and their associate to become a BO in smaller FIs. R.26 did not undergo a follow-up review. Since then, Armenia amended its legislation on the licensing of several categories of FIs. These changes are considered material. On this basis, R.26 is regarded as RUR.

Criterion 26.1 – All FIs are subject to the AML/CFT Law, with the CBA designated as sole competent supervisory authority (AML/CFT Law, Art. 10 (1)(8)). The CBA adopts secondary regulatory acts for FIs under its supervision, in relation to AML/CFT matters (CBA Law, Art. 3.1 (1)(d)).

Branches of foreign banks are explicitly included in the list of reporting entities in the AML/CFT Law or in the list of entities supervised by the CBA. For other sectors, branches of foreign FIs are considered REs and fall under CBA supervision where their operation is permitted under sectoral legislation, which defines the relevant FI types to include such branches (Securities Law, Art. 3(27), Investment Funds Law, Art. 1(1) and Art. 52(10), Insurance Law, Art. 8(4)). Where branches are not permitted under sectoral law, no such entities can operate in Armenia. At the time of the on-site, no branches of foreign FIs were registered or operational in Armenia. Opening a branch would require similar steps as licencing a local FI, ensuring oversight of CBA[107].

Criterion 26.2 – All FIs are required to be licensed by the CBA (Licencing Law, Art. 43(2)).

Core principle FIs: banks and foreign branches (Banks and Banking Law, Art. 4 and Art. 14(3)), credit organisations (Law on Credit Organisations, Chapter 2), insurance and reinsurance companies (Insurance Law, Chapter 7), investment companies (Law on Securities Market, Chapter 4), the Central Depository (Law on Securities Market, Chapter 18), investment funds managers (Law on Investment Funds, Chapter 9). Foreign branches of investment companies, investment managers and insurance companies need only to be registered by the CBA. However, the procedure, conditions and documents requested are consistent with the licensing process (Securities Law, Art. 43; Insurance Law, Art. 47; Investment Funds Law, Art. 60).

All others FIs: MVTS providers (Law on Payment and Settlement Organisations, Chapter 2), insurance brokers (Law on Insurance and Insurance, Chapter 17 and 18), pawnshops (Law on Pawnshops, Chapter 3), currency exchange offices (Law on Currency Regulation and Currency Control, Art. 7) and credit bureaus (Law on Credit Bureaus, Chapter 2).

Also, carrying out specific activities without a licence (including advertising as such) is specifically prohibited by sectoral legislation. (Banks and Banking law, Art 4; Law on Credit Organisations, Art. 3 (3); Insurance Law, Art. 39 (8); Law on Payment and Settlement Organisations, Art. 4(2); Securities law, Art. 33 (1); Investment Funds Law, Art. 8.1 (1); Law on Pawnshops, Art. 4; Law on Currency Regulation and Currency Control, Art. 7) and also by the Licencing Law (Licencing Law, Art. 46) for all types of licensed activities.

Conducting unlicensed activity is considered a crime (CC, Art. 281).

Shell banks are prohibited in Armenia (AML/CFT Law, Art. 15(2)). The definition of shell banks is in

[107] Supplementary legal interpretation given by the authorities as well as provisions in the Licensing Manual of the CBA highlighted the fact that if a foreign FI would consider opening a branch in Armenia, that branch would fall under the same legal requirements as a legal FI.

line with the FATF Standard (see c.10.1 – AML/CFT Law, Art. 3(39)).

Criterion 26.3 – Certain measures are in place to prevent criminals or their associates from holding (or being the BO of a significant or controlling interest, or holding a management function, in a financial institution. Any transaction of a direct or indirect "qualifying holding" is subject to a prior approval by the CBA, for banks, credit organisations, insurance companies, investment funds and investment funds managers, investment firms. The definition of a "qualifying holder" is similar for those types of entities and it refers to either the direct holder of more than 10% of the voting rights, or to the indirect holder, which includes any person, irrespective of the status or the level of shareholdings, who, in view of its business image or reputation, directly or indirectly is capable of predetermining the decisions of management bodies, significantly influencing their decision-making process (implementation), or predetermining the directions, spheres of activity of the FI, by virtue of this shareholding or by virtue of its right to claim against the respective legal person. (Banks and Banking Law, Art. 9; Credit Organisations Law, Art. 10(1(1)); Insurance Law, Art. 12; Securities Law, Art. 3(34)-(35); Investment Funds Law, Art. 8.3(2)).

Therefore, though there is no specific legal provision for the assessment of the beneficial owner, the definition of the indirect qualifying holder would cover the BO, irrespective of the type or chain of control, thus offering CBA the legal powers to assess and refuse the application, in reasoned cases, where the BO should be considered unfit.

The CBA has the legal powers to reject the application of individuals who have a record of conviction for an intentional crime (which has not been expunged or cancelled), or of those individuals that have committed an act, which in the opinion of the CBA provides ground for suspecting that the actions of the respective person as a member having the right to vote in the decision-making process of the highest management body of the FI, may result in the bankruptcy or worsening of the financial position of the bank, or harm the reputation and business image of the FI (Banks and Banking Law, Art. 18(1); Credit organisations Law, Art. 10(2); Insurance Law, Art. 18(1); Securities Law, Art. 55(1); Investment Funds Law, Art. 8.3(2))

In case of MVTSs and pawnshops, the legal provisions mention that any direct holder of more than 10% of the shares, or the BO, cannot be a criminal (LPSSO, Art. 20.1(1) (e1) -(e3); Law on Pawnshops, Art. 13(2)).

For currency exchange offices, the law is a little more lenient and provides for the exclusion of criminal only in case of direct shareholders that own more than 10% of voting right. However, BO and indirect holders can be rejected if CBA considers that acts committed by them, including criminal acts, might harm the reputation and business image of the organisation (Law on Currency Control, Art. 7^1 (6)-(7)).

Managers: the CBA has the powers to prevent criminals from holding managerial positions in all types of FIs. In case of banks, even the status of accused in criminal proceedings can be considered grounds for rejection (Banking Law, Art. 22, Art. 29 and Art. 33; Credit organisations Law, Art. 9.2, CBA Regulation 13, Chapters 13 and 21; Insurance Law, Art. 23.1, Art. 42.3 and Art. 51, Regulation 3/01 Chapters 18, 26, 27, Points 211(1), 216; Securities Law, Art. 51 and Art. 58; Investment Funds Law, Art 65; PSSPSO Law, Art. 22.2(2) and Regulation 17/01 Points 78 (2), 96(2, 3); Pawnshop Law, Art. 6 (h.1) and 13.1; Law on Currency Regulation and Currency Control, Art. 71(5) and CBA Regulation 10). The AML/CFT Law provides that the MLRO should have the status of senior manager, therefore, in this capacity, has to be considered fit and proper, with no criminal record (AML/CFT Law, Art. 24(6)).

The executive officers are registered without any time limitations to their tenure (lifetime registration) (CBA Banks Regulation 1, Point 201, Licensing Manual of FSLD). Only for members of the board of a bank, a five-year tenure is prescribed, after which the person shall be invited to an interview with the CBA to assess their professional competency (CBA Regulation 1, Chapter 29). Any subsequent changes (such as increase of shareholding, acquisition of qualifying holding, change of management) would trigger a fit and proper checks. The manual also requires for an annual re-evaluation of all managers, shareholders and UBOs.

There are provisions regarding affiliated persons, including requirements that applicants for a qualifying holding in a FI, or applicants for managerial positions, should not be affiliated with criminals.

The definition of affiliated persons includes members of the same family, or those that run a common household, or carry out joint business activity, or those that have been acting in agreement based on common economic interests, or they have been recognised as affiliated persons by a reasoned opinion of the Central Bank, which would cover close associates (Banks and Banking Law, Art. 8(2); Insurance Law, Art. 13(2), Securities Law, Art. 3(36), Investment Funds Law, Art. 3, last thesis). For pawnshops, exchange offices and MVTS, the legal provision redirects the definition of affiliated persons to that in the Banks and Banking Law (Law on Pawnshops, Art. 2; LPSSO, Art. 3(w); Law on Currency Regulation and Currency Control, Art. 7^1(6)).

Criterion 26.4 – The CBA can conduct off-site and on-site investigations of all FIs and groups (AML/CFT Law, Art. 29 and CBA Law, Art. 3.1, 5.1 and Chapter 5). For foreign branches and subsidiaries of Armenian FIs, supervision is conducted by the CBA based on MoUs signed with respective supervisors of the foreign jurisdictions. However, at the time of the onsite, no Armenian FIs had a foreign branch or subsidiary.

(a) The latest Financial System Stability Assessment (FSAP) report was published in 2018. As part of the FSAP process, an assessment of Armenia's compliance with the Basel Core Principles for Effective Banking Supervision and the IAIS Insurance Core Principles has been carried out. The results of the 2018 FSAP report are used as a basis for the assessment of this criterion.[108]

Basel Core Principles: the Basel Core Principles assessment found that, in general, the CBA has a well-structured banking supervisory regime and fully comply with the majority of the principles. Most of core principles were assessed as compliant. The assessment found that, in general, the CBA's responsibilities and powers are well established. Nonetheless, several FSAP recommendations were on the regulatory and supervisory framework. The prudential risk-based supervisory program appeared comprehensive and while gaps in supervisory information were identified, plans were directed towards addressing those areas (Core Principle (CP) 8). The extent of onsite validation inspections versus off-site analysis activities was considered to need better balance (CP 9). The laws and regulations were considered to provide the CBA with sufficient tools to address unsafe and unsound practices within a bank or domestic banking group in a timely fashion, nevertheless, enforcement needed to be strengthened (CP 11). As supervisory powers do not automatically apply to branches and subsidiaries of Armenian groups located outside Armenia, MoUs signed with foreign supervisors should be revisited (CPs 3 and 13).

IAIS Principles: In the absence of life insurance activities in RA, the insurance regulatory framework was not assessed.

IOSCO: No IOSCO assessment was provided. Nevertheless, the 2018 FSAP report mentions that CBA has been proactive in introducing frameworks for new instruments, and the overall regulatory framework for capital markets is sound (Para 49).

(b) Non-Core Principles financial institutions, including MVTS and currency exchange offices, are

108. Available at https://www.imf.org/en/Publications/CR/Issues/2018/12/12/Republic-of-Armenia-Financial-Sector-Assessment-Program-Press-Release-Staff-Report-and-46461.

subject to AML/CFT regulation and supervision by CBA (AML/CFT Law, Art.29 and CBA Law, Art. 3.1, 5.1 and Chapter 5).

Criterion 26.5 – The obligation of the CBA to adopt a risk-based approach for AML/CFT supervision, is prescribed in various regulatory and internal documents of the CBA ("Banks ML-TF risk assessment Methodology" and "Non-banks ML-TF risk assessment Methodology"). The CBA methodologies refer to banks, investment companies, credit organisations, central depositary and MVTS providers, and since very recently, to investment funds managers, pawnshops and currency exchange offices.

The authorities advise that all currency exchange offices should undergo a video inspection every three years, with more frequent surveillance performed when deficiencies are discovered. As the AML/CFT risk for pawnshops is minimal, inspections are conducted based on alerts.

The frequency and intensity of AML/CFT supervision for the rest of FIs is based on the individual residual ML/TF scores and included in an annual inspection plan. According to the Methodologies, FIs that get higher ML/TF residual risk scores are subject to more frequent inspections. Also, inspections may be conducted on matters not included in the annual plan if the need has arisen to assess newly emerging, unforeseen risks or based on FMC dissemination, findings as per quarterly reviews as well as information received from other sources (Section 9 of Banks ML-TF RA Methodology and Section 11 of Non-bank FIs ML-TF RA Methodology on inspection cycles for banks).

(a) The individual residual score depends on the level of inherent risk and quality of risk control framework. The CBA has developed an inherent risk assessment questionnaire to identify risks across customers, geography, transaction and products/services/delivery channels for the assessment of the quality of risk control framework for each FI. The questionnaire includes information on the FI's own risk assessment, risk appetite, AML/CFT trainings, independence and competence of the internal monitoring unit (including the money laundering reporting officer), oversight by the audit function (including the board and internal audit), CDD, automated transaction monitoring and screening systems, STR/CTR reporting procedures and group level procedures etc.). Additionally, FIs are required to submit supporting evidence and documents to endorse their responses included in the questionnaires (policies and procedures, training materials, internal audit reports, reports to the Board, minutes of the meetings etc.).

(b) The risk assessment process has to consider the threats and vulnerabilities identified in the ML/TF NRA (Paragraph 4 of the Banks ML-TF RA Methodology and paragraph 3 of the Non-bank FIs ML-TF RA Methodology). The frequency of inspection of banks, MVTS providers, investment firms and the Central Depositary depends on the risk level of each sector as identified the NRA. The findings of the NRA are incorporated in the Methodologies by attributing greater emphasis to elements of risks that are considered the highest in the NRA in the models of the methodologies.

(c) The assessment of inherent risks considers the individual characteristics specific of FIs (size, scope and scale of operations, complexity of services/products offered etc.). Also, the level of the inherent AML/CFT risk of banks may be slightly adjusted considering factors such as the bank's business model, growth dynamics, revenue generated from high-risk products/services, the bank's founders, managers and BOs, geopolitical factors or any other factors that might seem of impact.

In case of groups, the approach on supervision is based on a general level of risk at group level, considering prudential and conduct elements including analysis of intragroup transactions. Furthermore, as part of annual institutional risk assessment quality of group level policies and procedures is being assessed irrespective of inherent risk level (Banks ML-TF risk assessment Methodology, Table 11). In case of inherent low risk financial groups, no further supervisory action plan is developed. For medium, elevated and high inherent risk, an annual supervisory plan is developed (CBA Group Supervision Manual).

Criterion 26.6 – Individual risk assessments of banks, investment companies, investment fund managers, credit organisations, central depositary, pawnshops, exchange offices and MVTS providers are conducted, as a rule, annually. In addition, the inherent risk profile of banks is reviewed quarterly based on the data received by the CBA. The ML/TF risks may also be adjusted on an ad-hoc basis, where necessary, including in case of essential changes in the FIs management systems and business models, as well as in cases when other information and alerts are brought to the attention of the CBA (Banks Methodology, Clause 1, Point 8 and 9, Clause 8, Non-Banks Methodology, Clause 1, Points 8 and 9).

In case of financial groups, CBA evaluates the level of inherent risk based on a series of criteria laid down in the CBA Group Supervision Manual. Those include mostly prudential indicators which, although not explicitly mentioned, can accommodate ML/TF risk factors. The final inherent risk of the group is based on supervisory judgement, and falls into four categories, from Low to High. For groups that fall into the low-risk category, no other steps are performed, but the level of risk is re-evaluated annually. For groups falling into the other three risk categories, internal controls are assessed, and the level of residual risk is calculated based on a matrix. In addition to the general group risk assessment, internal controls developed at group level are evaluated during the individual risk assessment as long as they are applicable to the respective reporting entity. Ongoing monitoring is conducted at intervals predefined in the Annual Supervision Plan, or whenever the need arises.

Weighting and conclusions

Most of the R.26 criteria are met, but some minor shortcomings remain. No dedicated assessment of ML/TF risk is performed at the group level, but this is considered to have limited impact as the evaluation of applicable group-level internal controls and analysis of intragroup transaction are included in the individual risk assessment process. **Armenia is LC with R.26.**

RECOMMENDATION 27 – POWERS OF SUPERVISORS

In its 2015 MER, Armenia was rated C with R.27. No material changes have been introduced since then and the below analysis represents 2015 MER findings.

Criterion 27.1 – The CBA is responsible for the supervision of all FIs and has adequate powers to monitor compliance by all financial institutions with AML/CFT requirements. (CBA Law, Art. 3.1 para 2(d)), art. 5, para 1(e) and Chapter 5^{1}).

Criterion 27.2 – The CBA has the authority to conduct off-site supervision and on-site inspections of all financial institutions. Inspections are carried out by an authorised department of the CBA (FSLD). The CBA may examine the activity of supervised entities at the premises of the supervised entity or conduct a desk review at the CBA (CBA Law, Art. 39^{1}, paras 2, 4, 8.). The legal framework for conducting on-site inspections is comprehensive (e.g. access to the premises as well as to the server and computer software of the supervised entity, meeting executive managers/customers and/or participants as requested, obtaining of required information and documents, copies of required documents etc.) (CBA Law, Art. 39^{4}).

Criterion 27.3 – The CBA has the power to compel production of or obtain access to all relevant documents and information. The supervised entity must observe the lawful requirements of the inspection team, and must deliver explanations, information and clarifications, in writing or verbatim, to the inspection team regarding the documents and information subject to inspection. The inspection team is authorised to demand the necessary documents even if such documents contain banking, commercial or other secrecy. There is no restriction on the access to the relevant documents/information, and in particular there is no need for a court decision to get the relevant documents/information. (CBA Law, art. 39^{3} and $39^{4)}$).

Criterion 27.4 – Armenia has a wide range of administrative sanctions available to deal with natural as well as legal persons who fail to comply with the AML/CFT Law. There are sanctions available to cover all relevant obligations regarding Recommendations 6, and 8 to 23 (CBA Law, Art. 39[7]). The CBA has adequate powers to impose sanctions for failures to comply with the AML/CFT requirements. For AML/CFT breaches by banks, credit organisations, insurance companies, insurance intermediaries, investment companies, investment funds, pension fund managers, PSOs and pawnshops, the CBA can apply the following sanctions: issue warnings and directives or remedial sanctions to eliminate infringements; impose penalties/ fines; deprive managers' qualification certificates and revoke licences. For failures by money exchange offices, the CBA can issue warnings, impose fines and suspend/or revoke the licence. For failures by PSOs the CBA has the following sanctioning powers: issue warnings, require the institution to rectify infringements or to comply with the requirements; prohibit the activity of a PSO or, in case of a foreign PSO, withdraw its authorisation; demand the change of the Armenian PSO management, or terminate/ withdraw its authorisation; or impose fines.

Weighting and Conclusion

Armenia is C with R.27.

RECOMMENDATION 28 – REGULATION AND SUPERVISION OF DNFBPS

In its 2015 MER, Armenia was rated PC with R.28 based on the following deficiencies: very limited requirements for DNFBPs regarding measures to prevent criminals from being professionally accredited, or holding a management function in an entity or holding or being the beneficial owner of a significant or controlling interest, no legal basis to sanction directors or the senior management of DNFBPs except for the gambling sector, no risk based supervision applied to real estate agents, dealers in precious metals and stones, lawyers (apart from advocates) and law firms, accountants, TCSPs and advocates.

Since then, Armenia amended its legislation on risk-based supervision of DNFBPs and licensing requirements for online game of chance. These changes are considered material. On this basis, R.28 is regarded as a recommendation under review.

Criterion 28.1 -

(a) Casinos, organisers games of chance (including online), and lotteries are required to be licensed by the Ministry of Finance (MoF) (Licensing Law, Art. 43. Game of chance and casinos law, Art. 4 and 8. Lotteries Law, Art. 4). Operating a casino, game of chances or a lottery without a licence is a crime (Licensing Law, Art. 46 and CC, Art. 281). Additionally, engaging in illegal entrepreneurial activity is sanctioned by a fine in the amount of 15 to 30 times the minimum monthly wage (Administrative Code, Art. 169).

(b) *Significant participation, control and BOs*: Measures are in place to allow the MoF to prevent the following persons from holding more than 10% of the capital or being a beneficial owner of casinos, organisers of games of chance and lotteries: (i) persons who have been convicted for an intentionally committed crime, (ii) persons who were deprived by a court of the right to hold positions in financial, commercial, economic and legal areas; (iii) persons who cannot justify the origins of the funds invested in casinos, game of chance organisers or lotteries (iv) any participant of a casino, organiser of game of chance and lotteries whose license has been revoked in the past 3 years (Game of chance and casinos Law, Art. 2, Art. 4.1, Art. 4.2, Art. 8(2), Art. 14, Art. 15. Lotteries Law, Art. 2, 4.1 et Art. 4.2). There are no provisions regarding association with criminals.

Managers: same exclusions apply for applicants of managerial positions (Game of chances and casino Law, Art. 2 and 4.3. Lotteries Law, Art. 2 and 4.3). However, verification of those persons is performed after the appointment, within a time limit of 3 months, inside which the applicant is allowed to perform its duties, which is considered a shortcoming, though minor (Game of chance and casinos Law, Art. 4.3. Lotteries Law, Art. 4.2 and 4.3). Although there are no legal requirements for periodic checks on managers, there is a general provision that managers cannot be criminals or affiliates of criminals (Games of chance and casinos Law, Art. 4.1 (3); Lotteries Law, Art. 4.1 (3)). On the other hand, the managerial positions subject to checks are narrowly defined. For casinos, this applies only to directors, gambling hall manager and head of AML/CFT unit and for lotteries, only to head of executive body and head of AML/CFT unit (Games of chance and casinos Law, Art. 2, Lotteries Law, Art. 2, 7.1), which therefore, exclude other categories of managers.

(c) The SRC exercises supervision over casinos, organisers of games of chance and lotteries for AML/CFT compliance. The SRC conducts off-site supervision and on-site examinations (Game of chance and casinos Law Art. 9(1)). Monthly statements of financial flows are sent to the SRC by operators (Game of chance and casinos Law Art. 10). The SRC has the power to sanction for violations of the AML/CFT Law. It can issue warnings and assignments to rectify breaches, impose fines (Game of chance and casinos Law, Art. 9(1) 11(2) and Lotteries Law, Art. 11, AML/CFT Law, Art. 29.4). The MoF has the authority to suspend or revoke the license of casinos or organizers of games of chance in case of a breaches of relevant law (Game of chance and casinos Law Art. Art. 6(2) and Art. 9(1)).

Criterion 28.2 – In Armenia, each category of DNFBP has a designated AML/CFT supervisory authority. The FMC is responsible for supervising real estate agents, DPMS, law firms and sole practitioner lawyers (legal advisors), accounting firms and sole practitioner accountants and TCSPs (AML/CFT Law, Art. 29(1); the MoJ supervises notaries (Notary Law, Art. 19(1)) and the Chamber of Advocates is responsible for advocates (Advocacy Law, Art. 7(1)(4)).

Criterion 28.3 – All categories of DNFBPs[109] are subject to monitoring of compliance with AML/CFT requirements either by the CBA (through FMC), the MoJ or the Chamber of advocates (ChoA), to different degrees (AML/CFT Law, Art. 29(1) and (1.1)). In the case of advocates, the supervision is carried out by the ChoA, a self-regulatory body (SRB) which is not subject to oversight by any other competent authority.

Criterion 28.4 –

(a) The CBA (FMC) has adequate legal powers to supervise AML/CFT compliance (AML/CFT Law, Art. 29(1) see R.27).

The MoJ has adequate supervisory powers, including, the powers to investigate compliance with AML/CFT Law, carry on onsite and offsite controls and access to relevant information. (Notarial Profession Law, Art. 19 (1) and (2)).

The ChoA has limited powers to conduct monitoring of compliance with AML/CFT requirements. Its powers to carry out inspections are narrowed down to the context of disciplinary proceedings, which may be initiated upon receipt of external complaints or when a possible violation is identified in the course of exercising its other powers. (Advocacy Law, Art. 39.2(1)).

(b) No measures are in place to prevent criminals or their associates from being professionally accredited or licensed, or holding a significant or controlling interest, being the beneficial owner or holding a management function in the DNFBPs sector, except for advocates and notaries who cannot be persons convicted for deliberately committed crime (Advocacy Law, Art. 33, Notary Law, Art. 10).

(c) - Sanctions are available for failures to comply with AML/CFT requirements for all DNFBPs (AML/CFT Law, Art. 30(4) for legal persons and AO Code, Art. 165.9 for natural persons). The competent supervisory authorities are responsible for imposing sanctions: the MoJ for notaries and the CBA (FMC) for all other DNFBPS (CBA: AML/CFT Law, Art. 29(1) and AO Code Art. 165.9 and MoJ: Notaries Law, Art. 27.1). Advocates can only be subject to disciplinary liability imposed by the Disciplinary Commission of the ChoA, which may apply sanctions including reprimand, severe

109. Auditing firms are also covered by the AML/CFT Law, although they do not fall under the FATF definition of DNFBPs.

reprimand, additional training, fines and withdrawal of licence (Advocacy Law, Art. 11.1 and Art. 39.10). The range of available sanctions for AML/CFT failures of DNFBPs is however limited. There is no legal basis in the sector specific laws of the DNFBPs which empower the supervisory authorities/the authorised body to suspend or revoke a license for breaches of the AML/CFT Law. There is no legal basis to sanction directors or the senior management of DNFBPs (see R.35).

Criterion 28.5 –

(a) Provisions for the application of a risk-based approach in supervision are included in specific manuals (that include risk assessment methodologies), of some authorities. Notably, the MoJ and the CBA (FMC) have developed two such manuals: for notaries and for DNFBPs supervised by the CBA (FMC) (real estate agents, dealers in precious metals and stones, law firms & sole practitioner lawyers (legal advisors), accounting firms & sole practitioner accountants, TCSPs).

CBA (FMC): the manual requires CBA (FMC) to develop and to carry out individual inherent risk assessments for all entities, that should be based on several risk factors (customer, geographies and product, service risks and internal controls) and take into account the high-risk criteria provided by the AML/CFT Law and the NRA (PEPs, offshore jurisdictions notably) obtained through customised self-assessment questionnaires. Additionally, the CBA (FMC) assesses the quality of the internal control systems of each entity and establishes the residual risk level, that can be *low*, *medium* or *high*, dependent on which the intensity of supervisory activity shall be established (DNFBP Supervisory Manual, Clause 15).

For high-risk DNFBPs, on-site full scope or thematic inspections are to be conducted, while medium- and low-risk entities are primarily supervised through remote reviews or supervision meetings. The manual developed by the CBA applies to different categories of DNFBPs and stipulates that the risk assessment methodology should consider the characteristics of each DNFBPs, their diversity and number to determine the frequency and intensity of supervision.

Each year, a supervisory plan is adopted which takes into consideration the individual risk assessment results and prioritises high-risk DNFBPs. The supervisory methodology does not prescribe minimum inspection frequencies tied to risk levels; these are instead determined through the annual supervisory plan.

MoJ: The Control Department of the MOJ shall conduct individual risk assessments (Annex Notaries RA Methodology Point 1) based on the analysis of existing documents on notarial actions, information on the clients who are parties to notarial actions/on their activities, on analysis of characteristics of the transaction and on geography, classifying the notaries into *low*, *medium* or *high*-risk categories. However, while examples are given, there is no specific list of risk factors and other characteristics of the notaries, in particular their diversity and number to determine the frequency and intensity of supervision, are not considered. Also, there is no actual methodology provided, apart from the compulsory inclusion of some notaries into high-risk category based on certain provisions.

The frequency of conducting the risk assessment varies between one and three years depending on the previous risk score, with high-risk notaries assessed more frequently and mandatorily included in the inspection plan for the following year. Although it is mentioned that the risk assessment is performed for effective implementation of supervisory function in the AML/CFT area, there are no further provisions on how the level of risk influences neither the intensity, nor the frequency of supervisory activity.

SRC does not have in place a formal risk-based approach to supervision and rather uses its powers when needed and based on different triggers, including analysis performed by FMC.

Given its very limited powers, as stated in c.28.4, ChoA only acts in the form of disciplinary proceedings, upon complains. There is no evidence of risk-based AML/CFT supervision performed on the activity of advocates by their designated authority (ChoA).

(b) Both the CBA and the MoJ use the risk manual to define the supervisory planning. DNFBPs under CBA (FMC) are risk modelled with residual risk scores as mentioned above.

Apart from that, the manual adopted by the MoJ makes no reference to the assessment of internal controls, policies or procedures of notaries.

When analysing the data provided through these questionnaires, additional criteria defined by the Manual are also considered by the CBA. These include, in particular, the share of the relevant group of DNFBPs in the domestic market, their activity in international markets, the results of NRAs and other strategic analyses conducted by FMC, surveys from state bodies, publications from reputable international organisations, media reports, including indications of involvement in crimes, statistical data on ML/TF efforts, and the level of awareness among DNFBPs regarding ML/TF/PF measures, although it is not clear how those are quantified in the final score (DNFBP Supervisory Manual, Clauses 5, 6).

Apart from the provisions in the law and secondary legislation regarding low risk factors, there is no degree of discretion allowed to REs.

Weighting and conclusions

While methodologies for risk assessment and manuals for conducting supervisory activities have been developed for some DNFBPs, such as notaries and those under the FMC's area of supervision, there is a lack of clear provisions laying down rules for adapting the intensity and frequency of supervisory activities to the level of risk, especially for some more material sectors such as casinos and gambling operators. Not all authorities have the adequate powers to conduct inspections. The range of available sanctions for AML/CFT failures of DNFBPs is limited. There are limited requirements for DNFBPs regarding measures to prevent criminals from being professionally accredited or holding a management function in an entity or holding or being the beneficial owner of a significant or controlling interest. **Armenia is PC with R.28.**

RECOMMENDATION 29 - FINANCIAL INTELLIGENCE UNITS

In its 2015 MER, Armenia was rated C with R.29. No material changes have been introduced since then, and thus, the below analysis represents 2015 MER findings. Nevertheless, minor amendments have been introduced that pertain to updating relevant references to the legal acts and/or the most current strategic analyses, etc.

Criterion 29.1 – The Financial Monitoring Center, which serves as the Armenian FIU, is a structural unit established within the Central Bank of Armenia. It acts as a national center for receiving and analysing suspicious transaction reports (STRs) and other information relevant to ML/TF and associated predicate offences, and for disseminating the results of that analysis (AML/CFT Law, Article 10; FMC Statute, Chapter 1, Chapter 2 Clause 6.1).

Criterion 29.2 – The FMC is the central agency for the receipt of disclosures filed by reporting entities, including: 1) STRs filed by reporting entities as required by R.20 and R.23; and b) TTRs (threshold transaction reports) filed by reporting entities according to certain types of transactions and thresholds, including reports on cash-related transactions, reports on transactions involving real estate, reports on transactions related to managing of client property, bank and securities accounts, etc. (AML/CFT Law, Parts 3-4 of Article 6; Part 1 of Article 10). A TTR is to be submitted to the FMC within three working days of concluding the transaction, whereas in the case of an STR it is to be submitted within the same working day or, if it is not possible (these cases are indicated by the Guidelines), before noon of the following working day.

Criterion 29.3 – The AML/CFT Law empowers the FMC to request from any reporting entities (even those which had not submitted an STR) additional information relevant to the purposes of the AML/CFT Law, including classified information as defined by the law (Clauses 2 and 4 in Part 1 of Article 10; Part 5 of Article 13 of the AML/CFT Law). As it was mentioned above, the main technical deficiency identified in the 3rd MER was an ambiguity on whether the obligations of the AML/CFT Law override the secrecy provisions and permit the provision of additional information with regard to lawyers, accountants and auditors. Armenia addressed this deficiency by amending the AML/CFT Law which now provides that information should be provided regardless of confidentiality (Clauses 2 and 4 in Part 1 of Article 10; Part 5 of Article 13 of the AML/CFT Law).

In addition to data and information within its database, the FMC has direct and indirect access, through MoUs signed with state authorities, to a wide range of administrative, law enforcement, financial and other information that it requires to properly undertake its functions.

Criterion 29.4 – The FMC undertakes operational analysis based on the information received from reporting entities and the other information available to it (as described in the analysis for Criterion 29.3). The analysis is aimed at identifying specific targets, following the trail of particular activities or transactions and determining links between those targets and possible proceeds of crime, ML/TF and predicate offences.[110] The FMC uses the Automated Case Management System (ACMS) that has analytical and data processing functions and provides tools for both operational and strategic analysis. The ACMS has been assessed and found compliant with the FIU Information System Maturity Model (FISMM) of the Egmont Group. FMC is also required to undertake strategic analysis and over the period 2020-2024 has issued typology studies and a number of strategic analysis reports including the 2021 ML/TF NRA; the 2021 PF NRA; the 2024 and the 2024 ML/TF NRA. FMC has three staff members assigned to carry out strategic analysis of ML/TF trends and patterns regularly.

Clauses 6.2 in Chapter 2 of the FMC Statute establishes that one of the FMC's tasks is the performance of strategic assessments for the purpose of identifying and preventing ML/TF/PF risks, including the conduction of national risk assessments. In accordance with Clause 7.15 of the Statute, the functions of the FIU encompass the organisation of activities for performing national risk assessments on ML/TF/PF and collecting and analysing data on high ML/TF/PF risks and their periodic occurrences (methods, schemes) or trends, by developing and publishing high risk and suspicious criteria/typologies based on the results of the analysis. Section 6 of the FMC Operational Manual further sets out the process for the preparation and conduction of strategic analysis.

Criterion 29.5 – The FMC is authorised to disseminate (spontaneously or upon request) the results of operational analysis, in the form of a notification as well as additional data related to the circumstances described in the notification, to criminal prosecution authorities (Parts 3 and 4 of Article 13 of AML/CFT Law). Information disseminated by the FMC is classified and handled in accordance with the relevant CBA procedures (Section IV of the FMC Operational Manual). A notification or a response by the FMC to an inquiry to competent domestic authorities is processed within the Automated Case Management System. This and other information exchange is conducted via a dedicated network "Financial Intelligence Data Exchange Platform" (with no Internet access) which provides competent authorities with a secure and protected communication channel.

Criterion 29.6 –The FIU is required by law to keep confidential any information received, analysed or disseminated by it. For such purpose, there are detailed internal procedures in place for the handling, storage, protection of, and access to, information contained in the FIU's IT system, which can only be accessed by FIU staff (Parts 7-8 of Article 10; Article 12 of AML/CFT Law). In 2023 the CBA was

110. Clause 2 in Part 1 of Article 10 of AML/CFT Law; Clauses 6.1 and 7.2 in Chapter 2 of the FMC Statute; Section III of the FMC Operational Manual

assessed and found fully compliant with the ISO Standard 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements Standard).

Criterion 29.7 – The following factors are relevant to FMC's operational independence and autonomy.

(a) FMC is a "responsible structural unit" within the CBA but acts with operational autonomy and independence (Parts 1-6 of Article 10 of the AML/CFT Law). The head and the staff members of FMC are appointed by the Board of the CBA (as opposed to other CBA staff) which also oversees FMC by approving its statute, the annual operations plan, and the budget (FMC has a separate budget). The Board of the CBA also decides upon application of responsibility measures[111] for AML/CFT violation by legal persons and reporting entities that have no supervisory authority in the field of AML/CFT All operational decisions (incl. the power to suspend suspicious transactions and business relationships and matters such as specific STRs, or other sources of information which are to be disseminated by FMC on a strictly technical basis, are left to FMC sole discretion.

(b) FMC is able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information. For this purpose, it may conclude agreements of co-operation with foreign counterparts (Part 1 of Article 13; Parts 1, 2 and 4 of Article 14 of the AML/CFT Law; Clauses 6.1-6.4, 7.1- 7.3, 7.5-7.6, and 11-12 of the FMC Statute).

(c) FMC has legally established core functions (Parts 1-6 of Article 10 of the AML/CFT Law; Clauses 1-2, 7.1-7.6, 11 and 14 of the FMC Statute; Sections I- IV of the FMC Operational Manual).

(d) FMC is able to obtain and deploy the resources needed to carry out its functions, on an individual and routine basis, free from any undue political, government or industry influence or interference. The FMC staff (both the management and the operational level) is assigned and dismissed by the CBA Board (the highest collegial management body of the Central Bank). The FMC has a distinct budget within the CBA budget, which provides for covering both operational and administrative expenses, as well as capital expenditures. The FMC staff has increased since the last evaluation and comprises about 38 persons. The FIU is equipped with technical resources necessary for the proper implementation of its functions (computers, printers, etc.). High professional standards of the FIU staff are ensured by requirements set out in the Labour Code, job descriptions established for each job position and the FMC Code of Conduct and the CBA Code of Conduct which sets outs professional and ethical standards for its employees (Parts 3 and 5 of Article 10 of the AML/CFT Law; Clauses 9, 13,-16-17 and 19 of the FMC Statute).

Criterion 29.8 – the FMC obtained the status of a member of the Egmont Group during the Egmont Group Plenary Session on March 29, 2007.

Weighting and Conclusion

Armenia is C with R. 29.

RECOMMENDATION 30 – RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

In its 2015 MER, Armenia was rated LC with R.30, based on the fact that the authorities did not routinely pursue pro-active parallel financial investigations. R.30 did not undergo a follow-up review. The FATF Standards for R.30 have undergone a revision against which the country has not previously been assessed. On this basis, R.30 is regarded as a recommendation under review (RUR).

Criterion 30.1 – Following the adoption of the new CPC in 2021 and its subsequent amendments, organisational reforms have reshaped the intelligence gathering and investigative system. Various authorities have taken responsibility for investigating ML at different stages during the period under

111. Defined under AML/CFT Law and the Code of Administrative Violations.

review. From 2015 until October 2021, the National Security Service (NSS) held exclusive authority over ML investigations. As of January 2023, the Investigative Committee (IC) has taken over as the primary body responsible for ML investigations, with the Anti-corruption Committee (ACC) having competence for ML investigations related to corruption. The IC rely on the intelligence gathering activities performed by the National Security Service (NSS), the State Revenue Committee (SRC) and the Ministry of Internal Affairs (MIA). The AC primarily relies on intelligence activities conducted by its subordinate operational intelligence units regarding corruption-related offences, including money laundering (CPC, Article 181, CC, Annex 1).

The investigation of TF is under the competence of the IC (CPC, Article 181(2)). At the beginning of the assessment period, both the NSS and the IC were responsible for investigating TF, but following a government decree in 2024, the investigative arm of the NSS was absorbed into the IC.

In exceptional cases, the Prosecutor General has the authority to transfer the criminal proceedings to another preliminary investigation body, where this is necessary as a last resort in order to ensure conduct of impartial preliminary investigation. (Article 181(8) of CPC).

Criterion 30.2 – Although the CPC does not expressly authorise the LEAs entrusted with the investigation of predicate crimes to pursue parallel financial investigations, according to the explanation provided by the authorities, the financial investigation is performed alongside or in the context of a standard criminal investigation of predicate crimes. The ML and TF investigation Guidelines indicate that investigating authorities shall focus on the predicate crime and ML in parallel (ML Investigation Guide, Chapter 2 (a)). The two investigative bodies IC and ACC have powers to pursue the investigation of a related ML offence: IC in connection to the standard investigation of any predicate crime, and the ACC in connection to corruption-related offences. The investigation of any related TF offence will be pursued only by the IC (CPC, Article 181).

Criterion 30.3 – The IC and the ACC have the authority in identifying and tracing criminal property and property of corresponding value related to crimes under their competence and may apply the available investigative techniques provided by the CPC and the LOIA (CPC, Chapters 28-31; LOIA, Article 14). The IC may also instruct the inquiry bodies (MIA, NSS and SRC) to perform undercover investigative action and operative intelligence measures and ask for their support during the performance of evidentiary and other procedural actions, including the identification and tracing of criminal property. The ACC can rely on similar support from its own investigative unit (CPC, Article 41(1)(10)(12)). The seizure of property is initiated based on the decision of the investigator, subject to court approval, and extends to property of corresponding value (CPC, Article 131(1), 133; Chapter 15 *Attachment of property*) (see R.4, c.4.4). Nevertheless, concerns remain regarding the timely access to a wide range of information necessary to support the identification and tracing of criminal property and property of corresponding value, in particular, due to the insufficiently broad access to banking and similar information, as well as limitations in timely access to information on natural and legal persons' bank accounts (see R.31 c.31.1(a) and 31.3 (a)).

Criterion 30.4 – Armenia does not have other competent authorities which are not LEAs, but which can pursue financial investigations of predicate offences.

Criterion 30.5 – The ACC, as the responsible investigative authority for corruption-related offences, has equal authority to identify, trace, and seize assets.

Weighting and Conclusion

The responsibilities of LEAs are largely in line with the requirements of R.30. Concerns remain regarding the timely access to a wide range of information necessary to support the identification and tracing of criminal property and property of corresponding value described under R.31 c.31.1(a) and 31.3 (a)) (c.30.3). **Armenia is LC with R.30.**

RECOMMENDATION 31 - POWERS OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES

In its 2015 MER, Armenia was rated PC with R.31, based on the following deficiencies: legal limitations impact on (i) LEAs powers to use compulsory measures for production of records; and (ii) the range of investigative techniques available for investigations. R.31 did not undergo a follow-up review. The FATF Standards for R.31 have undergone a revision against which the country has not previously been assessed. On this basis, R.31 is regarded as a recommendation under review (RUR).

***Criterion 31.1* –**

(a) *The production of record held by FIs, DNFBPs and other natural or legal persons:* The powers to use compulsory measures for the production of records held by FIs, DNFBPs and other natural or legal persons are limited.

The power to request information when there are sufficient grounds to assume that it may result in obtaining significant evidence for the criminal proceeding is not compulsory in all cases (CPC, Articles 208(1) 8), 209(1)). Natural or legal persons may refuse requests to provide information containing attorney, notary, banking or related secrecy (CPC, Articles 170(3), 232(2) 1)). The refusal may also be based on a reasonable belief that the information could be used or interpreted to the person's detriment, their spouse or close relative (CPC, Article 232(2) 3), 4)).

There is no compulsory production power in relation to records containing *notary, banking or related secrecy*. Such information may be obtained pursuant to a court-ordered seizure, which involves entry into the premises where the seizure is to be carried out. In the event of refusal, investigators are authorised to perform searching actions of the premises (CPC, Article 209(4)5) (6)(8)).

The power to seize information is limited in scope and does not provide sufficiently broad access to *all necessary documents and information* relevant for the investigation, prosecution or related actions involving ML, associated crime or TF. In case of natural persons, documents and objects containing banking or related information may be seized only in cases the information relates to (i) the *suspect* or *accused*; or (ii) a natural person reasonably believed to have a *direct connection with the suspect or accused*. This excludes persons in respect of whom no sufficient evidence has been gathered to consider them suspects, as well as persons with no direct link to the suspect or accused. In the case of legal persons, the power is even more restrictive, as it applies only to information related to legal persons whose activities are, fully or in relevant part, managed, controlled or otherwise the facto directed by the suspect or accused, thereby excluding all other legal persons (CPC, Article 239(4)).

(b) *The search of persons and premises*: Search powers are applicable both to places and persons and may be conducted with the view to find objects, substances, documents or data, including digital data and property subject to seizure (Article 234-237 of the CPC). The search of home, digital search and in other cases envisaged by the CPC, requires a court decision. In other cases, the search can be carried out based on the decision of the investigator (Article 209(2)(3) of the CPC).

(c) *Taking witness statements*: LEAs may conduct questioning of a witness, a victim, the accused, or of an expert. They can also conduct investigative actions of confrontation and checking testimony (Articles 209, 221-225 of the CPC).

(d) *Seizing and obtaining evidence*: seizure of objects, substances, digital data or documents are available to LEAs for investigating crimes under their mandate (Articles 208, 239 of the CPC).

Criterion 31.2 – Competent authorities have access to a wide range of investigative techniques for the investigation of ML, associated crimes and TF under the CPC and LOIA, including undercover investigative actions, operational intelligence measures, intercepting communications, assessing computer systems and controlled delivery (CPC, Chapters 30, 31 on *undercover investigative actions*;

LOIA, Article 14 on *types of operational intelligence* measures; CPC, Articles 248 and 249 on *monitoring non-digital and digital communications*; LOIA, Articles 25 and 26 on *interception of communications and wire-tapping*; CPC, Article 236 on *digital search*; LOIA, Article 19 *controlled supply and purchase*). The SRC can apply 9 out of 16 operational intelligence measures under LOIA, some of which can be important for their intelligence gathering activities related to tax and drug- related crimes (e.g. ensuring access to financial data and secret monitoring of financial transactions, LOIA, Art. 14(1)15)) (LOIA, Article 14 (4), (5)).

The scope of application of the available investigative techniques remains limited. The undercover investigative actions under CPC and the four operational intelligence measures related to internal surveillance, interception of correspondence, wiretapping and monitoring of financial transactions, may be applied solely in cases involving alleged serious or particularly serious offences[112] (with the exception of undercover actions in bribery-related proceedings) (CPC, Article 242(3); LOIA, Article 31(4)). As a result, the ML and TF offences, when not accompanied by aggravating circumstances, fall outside the scope of these measures. This limitation extends as well to a wide range of associated predicate crimes, even when accompanied by aggravating circumstances.[113]

Criterion 31.3 – (a) *Mechanism to identify whether natural or legal persons hold or control accounts*: A centralised bank account registry is maintained by the CBA (CBA Law, Article 35.1). However, there are concerns regarding the timely access to this information by investigative bodies. A request for information shall be responded by the CBA within 30 days, or within a longer period, if deemed necessary (AML/CFT Law, Article 13(4)).

Financial data may be accessed through monitoring of financial transactions (LOIA, Articles 14(1)(15) and 29). This operational intelligence measure may be applied only by the Police and the National Security Body (NSS) and is not available for the SRC (customs and tax authority) (LOIA, Article 14(2)-(5)). Additional restrictions apply – the measure may be employed solely in cases involving a suspicion of a serious or particularly serious offence. As described under c.31.2, this would exclude the ML and TF offences when not accompanied by aggravating circumstances, as well as a wide range of associated predicate crimes (LOIA, Article 31(4)).

Monitoring of financial transactions can also be carried out as an undercover investigative action (CPC, Article 250). Nevertheless, the measure may be applied: (i) only in relation to alleged serious and particularly serious crime, with the exception of the bribery-related proceedings, which imposes the same limitations as described above; and (ii) only in relation to the person suspected, accused, person with a *direct connection* with the suspect or the accused or a legal person whose activities are managed, controlled or directed by the suspect or accused (CPC, Articles 242(3), 243).

(b) *Process to identify assets without prior notification*. An investigator may issue a decision to carry out verifications whether a person possess any property, without prior notification (CPC, Article 41(1) 28)). The owner is notified only after a decision on the seizure of property is made and delivered to them. Specifically, pursuant to Article 133(4) of the CPC, the investigator serves the decision on seizure of property to the owner or possessor against signature and requires them to hand over the property subject to seizure. LEAs and PO have access to legal ownership information for joint stock companies held by the Central Depository (Securities Law, Article 98(2)(6)). Access to the basic and BO

[112]. Serious criminal offences are defined as acts punishable by a maximum of up to 10 years of imprisonment; particularly serious offences are those punishable more than 10 years or life imprisonment; offences of medium gravity are acts punishable by a maximum of up to 5 years of imprisonment, while those of minor gravity – a maximum of 2 years of imprisonment or a non-custodial punishment (CC, Article 17).

[113]. E.g. Article 268 *Use of inside information not in good faith*; Article 269 *Abuse of priced in the securities market*; Article 272 (1)(2) *Receiving a bribe in private sector*; Article 273 *Giving a bribe in private sector*; Article 281 *Illegal Entrepreneurial Activity*; Article 282 (1)(2) *Creating, organising or management a financial pyramid*; Article 290 (1) *Tax offence*; Article 291(1)(2) *Smuggling of Cash and/or payment instruments*.

information held in the State Register of legal persons is ensured on the basis of a concluded agreement (remains to be confirmed which investigative authorities have concluded such agreements, see c.24.9). Access to the information held by FIs and DNFBPs can be obtained through the FMC (see also c.24.9).

Criterion 31.4 – LEAs are authorised to ask for relevant information held by FMC when investigation of crimes under their mandate (Article 13 (4) of the AML/CFT Law).

Weighting and Conclusion

Competent authorities have powers for conducting investigations of ML, associated predicate offences and TF. However important shortcomings remain: (i) the measures for production of records are not compulsory in all cases, particularly in relation to banking and related information, while the power to seize such information is limited in scope and does not provide sufficiently broad access to all necessary documents and information (c.31.1(a)); (ii) the available investigative techniques cannot be used in all investigations of ML, associated predicate offences and TF due to their limited scope of application (only to serious and particularly serious offences) (c.31.2); (iii) no timely access in all cases to a wide range of information to support the identification and tracing of criminal property and property of corresponding value (c.31.3). **Armenia is PC with R.31.**

RECOMMENDATION 32 – CASH COURIERS

In its 2015 MER, Armenia was rated C with R.32. The recommendation did not undergo a follow-up review. Since then, a new Eurasian Economic Union (EAEU) Customs Code has entered into force on January 1, 2018, which establishes the declaration requirements to cross-border transportation of cash and monetary instruments across the borders of the EAEU. It is applicable to Armenia due to its membership (since 2015) of the EAEU, which also includes the Russian Federation Belarus, Kazakhstan and Kyrgyzstan. These changes are considered material. On this basis, R.32 is regarded as a recommendation under review (RUR).

Criterion 32.1 – Armenia implements a written declaration system for the incoming and outgoing cross-border transportation of cash and monetary instruments (BNIs), when these are intended for *personal use*[114] (EAEU Customs Code, Article 260(1) (7)(8)(10); Article 2(1) (3)(5)). The obligation to declare applies in cases where cash and BNIs are physically transported by a natural person crossing the borders of the customs union, when moved via international postal items, or when transported by a carrier (EAEU Customs Code, Article 256(3)).

When cash and BNIs are transported for purposes other than personal use, according to the authorities' explanations, they are subject to the requirement of submitting a commodity declaration in the form established by the Decision of the Customs Union Commission of 20.05.2010 No. 257 (EAEU Code, Article 105(3)).

The definition of *monetary instruments* is broad enough to comply with the definition of BNIs provided by the FATF Glossary. It includes traveller's cheques, bills of exchange, cheques (bank cheques) and certified securities which certify the obligation of the issue (debtor) for payment of funds, and which do not indicate the person such payment is made to (EAEU Customs Code, Article 2(1) (8)).

The declaration system applies only to transportation of cash and BNIs across the customs border of the Union (EAEU Customs Code, Article 2(1) (3)(5)). This means that only movements that cross the external borders of the EAEU are subject to the declaration requirements. There are no domestic provisions to address this gap. The authorities noted that Armenia does not share a physical border with

[114]. "Goods for personal use" means goods intended for the *personal, family, household and other needs of natural persons non-related to business operations* which are moved across the customs border of the Union as part of accompanied or unaccompanied luggage, by way of their shipping as international postal items or by any other means (EAEU Customs Code, Article 2(1) (46)).

other EAEU member states, while at the international airport, general border and security controls are implemented, which is viewed as a mitigating measure for this shortcoming.

Criterion 32.2 – Armenia has in place a written declaration system, which requires all travellers carrying cash and traveller's checks intended for personal use, when the total amount exceeds USD 10 000 or equivalent, to fill out a passenger custom declaration form when crossing the border of the EAEU. Other monetary instruments intended for personal use must be declared regardless of the amount (EAEU Customs Code, Article 260(1)(7)(8)).

In cases where the total amount of transported (one-time) cash and/or BNIs monetary instruments exceeds the equivalent of 100 thousand USD, the declaration must be followed by a submission of documents confirming their origin (Decision no. 130 of August 6, 2019, of the Board of the Eurasian Economic Commission).

Criterion 32.3 – Armenia applies a declaration system.

Criterion 32.4 – Upon discovery of an incomplete or inaccurate customs declaration, or in the event of failure to comply with declaration obligations, customs officials are authorised to request additional information necessary to establish the reliability and completeness of the presented information/documents, such as commercial and accounting records, relevant documents and data, including written explanations (EAEU Customs Code, Art. 325(4)).

Criterion 32.5 – Failure to fulfil customs declaration obligations (including declaring incorrect/false data, presenting invalid, forged documents) shall be punishable under the legislation of the member states of the EAEU (EAEU Customs Code, Article 84(3)). Armenia has in place two types of sanctions for failure/false declaration: administrative and criminal.

The administrative liability applies in case of i) illegal transportation of cash or payment instruments in small amounts across the borders of the EAEU; ii) hiding or failing to declare relevant information about them; iii) declaring information under a false name; iv) violating the rules for their transportation; v) fraudulently using customs or other documents. The amount is considered small when the value exceeds the equivalent of USD 10 000 and is less than the equivalent of USD 20 000. Such conduct may result in a fine amounting to ten percent of the sum of the illegally transported cash or the nominal value of the illegally transported payment instruments, which is calculated after the deduction of the amount permitted to be transported without declaration (i.e. USD 10 000) (Article 314(1)(2) Law on Customs Regulation, Article 291(4) CC). The established administrative penalty does not appear to be proportionate.

The commission of the same acts in relation to large amounts (exceeding the equivalent of USD 20 000), is subject to criminal sanctions (Article 291 CC). There is a wide range of criminal sanctions available, allowing the authorities to impose proportionate measures. These include: a fine in the amount of ten-fold to thirty-fold (approximatively from EUR 1 660 up to EUR 5 000); public works up to 200 hours; deprivation of the right to hold certain positions or exercise certain activities for a term of two to five years; restriction of liberty up to three years; short-term imprisonment for up to two months; imprisonment for a term of up to three years. Where aggravated circumstances exist, imprisonment for a term of two to six years may be applied, which is assessed as proportionate and dissuasive sanction.

Criterion 32.6 – The State Revenue Committee (SRC) shall provide the Financial Monitoring Centre (FMC) the following information obtained through the declaration process: 1) information on the cases of imported and exported cash, treasury bills, travel checks exceeding USD 10 000 – on a quarterly basis; 2) information on the cases of violating the declaration obligations/requirements – monthly; 3) information on the transit of bearer shares – monthly; 4) cases of ML/TF suspicions – within 4 days (FMC-SRC MoU, §7).

Criterion 32.7 – The co-operation between the SRC and the FMC is based on the Memorandum of Understanding concluded in 2017 in order to facilitate the implementation of the tasks and powers provided under the AML/CFT legislation. The Interagency Committee also serves as a platform for co-operation between the SRC and other authorities. The Migration Service is under the MIA, which part of the Interagency Committee, thus ensuring a platform for cooperation with the SRC.

Criterion 32.8 – Customs authorities have the power to stop or restrain currency or BNIs in cases of a ML/TF suspicion or false/non-declaration on the basis of information provided by the LEAs and the FMC (EAEU Agreement on movement of cash, Article 3). The authorities consider the SRC to be a LEA and, such, view these provisions as applicable to its powers. Under domestic legal provisions, the SRC has such powers to retrain goods, including cash, which are related to a custom violation (Law on Customs Regulation, Art. 327(1); Law on administrative violations, Art. 267(1)). The grounds for temporary suspension under the EAEU Agreement, for a period of up to 30 days, appear to be sufficiently broad to cover both false declaration and ML/TF suspicions (EAEU Agreement on movement of cash, Article 4).

Criterion 32.9 – Documents necessary for customs control, including those submitted with the custom declaration, must be stored for a period of 5 years (EAEU Customs Code, Article 320). Information on false and non-declarations and on ML/TF suspicions is submitted by the SRC to the FMC and is retained by the FMC for a period of no less than 5 years (FMC-SRC MoU, §7.1(b) (d); FMC Operational Manual, para. 62).

Criterion 32.10 – The information collected pursuant to the EAEU customs declaration obligation is subject to confidentiality: it can only be used by the customs and other state authorities to carry out their tasks and functions and in compliance with secrecy laws in force (EAEU Customs Code, Article 356).

Criterion 32.11 – Persons transporting cash/BNIs related to ML/TF or predicate offences are subject to criminal sanctions established for ML and TF offences or for smuggling of cash and/or payment instruments offence under Article 291 of the CC, which are considered proportionate (see c.32.5). The confiscation and provisional measures referred to in R.4 are applicable to the persons carrying out physical cross-border transportation of currency or BNIs related to ML/TF or predicate offences.

Weighting and Conclusion

Most of the criteria are met or mostly met. Some minor shortcomings remain: (i) only movements that cross the external borders of the EAEU are subject to the declaration requirements (c.32.1); and (ii) there are concerns regarding the proportionality of the administrative sanctions for false or non-declaration (c.32.5). **Armenia is LC with R.32.**

RECOMMENDATION 33 – STATISTICS

In its 2015 MER, Armenia was rated C with R.33. Since then, Armenia introduced significant changes regarding the substance of the statistics, the procedure and time limits for their submission to the FMC by several state authorities. These changes are considered material. On this basis, R.33 is regarded as a recommendation under review (RUR).

Criterion 33.1 – The requirement for state bodies to gather specific statistics concerning on matters relevant to the effectiveness and efficiency of their AML/CFT systems is embedded in the AML/CFT Law, secondary legislation – the FMC Rules on Statistics and the FMC Operational Manual.

(a) The FMC's *Operational Manual* requires statistics are kept on the number of STRs received from the reporting entities and on notifications sent to domestic competent authorities.

(b) In accordance with Article 13(8) of the AML/CFT Law, state bodies submit to the FMC statistics on the number of investigations, prosecutions and judgements (acquittals and convictions) on ML/FT. The data also includes the number of investigations which were concluded without charges being brought and the reasons for not instituting criminal proceedings.

(c) The same provision requires the authorities to register the value of arrested or seized property in the course of ML/FT investigations and (in the case of convictions) the penalties imposed and the value of confiscated property. The FMC Rules on Statistics from 2023 require further information to be provided, in particular information on confiscation imposed by court and actually confiscated for predicate offences to ML, property actually placed under arrest and further subject to confiscation for ML/TF cases and the values of property placed under arrest, confiscated, as well as property returned and distributed due to requests and motions on providing legal assistance received in criminal proceedings initiated with respect to cases of predicate crimes for money laundering.

(d) MLA for both incoming and outgoing requests concerning ML/TF are recorded on the basis of Article 13(8) of the AML/CFT Law. The FMC Rules on Statistics further specify the data collected on requests and motions on providing legal assistance (incl. extradition) sent and received in criminal proceedings initiated with respect to money laundering, associated predicate offence and terrorism financing cases. As for FIU information exchange with foreign counterparts, the FMC Operational Manual requires data on requests sent and received from foreign FIUs to be collected. No information was provided concerning the basis for collecting statistics on LEA international requests for co-operation made and received.

Weighting and Conclusion

There are minor shortcomings concerning the collection of statistics. There is no obligation for authorities other than the FIU to maintain statistics on informal information exchange made and received in the course of international co-operation. **Armenia is LC with R.33.**

RECOMMENDATION 34 – GUIDANCE AND FEEDBACK

In its 2015 MER, Armenia was rated as C with R.34. Since then, material changes have been introduced mainly relating to the issuance of guidance papers and trainings. On this basis, R.34 is regarded as a RUR.

Criterion 34.1 – In accordance with Article 10 (1)(13) of the AML/CFT Law the FMC provides on regular basis feedback to reporting entities on submitted STRs. It delivers on an annual basis detailed, written feedback in a predefined form on the quality of each STR, including on its format and content and information on the further use of the information received. In addition, FMC provides case-by-case verbal feedback and holds ad-hoc meetings as needed.

The authorities have organised a series of training initiatives in the last two years aimed at the AML/CFT legislative framework, targeted financial sanctions and the results of the national risk assessment. The vast majority of these trainings was dedicated to FIs.

In addition, a number of events and discussions were held to ensure the proper performance of notaries' duties within the framework of the fight against ML/TF/PF). Training courses for notaries were organised at the "Academy of Justice of the Republic of Armenia" SNCO (2023) and by the Council of Europe (2025).

The AML/CFT Law Article 10 (1)(6& 7) also sets out the legal basis for the issuance of a large variety of guidelines and secondary legislation (regulations) in the field of AML/CFT. The CBA has published several such documents on its website, inter alia the Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing; Guidance on Suspicious Transaction Criteria, Freezing Guidance; BO Guidance; High risk and suspiciousness criteria for terrorist financing and proliferation financing (for the implementation of TFS) and ML typologies and analyses of different ML schemes. While the majority of ML typologies were published prior to the period under review, in June 2025 three new typologies were published.

Under AML/CFT Law Article 10 (1)(6) the FMC issues assignments to ensure specific categories of reporting entities' proper implementation of AML/CFT provisions. These include inter alia assignments on topics such as: the process and results of identifying the transaction or business relationship as suspicious, establishing non-face-to-face business relationships, cash transactions, management of risks related to cross-border transactions, strategic risk analysis of money laundering, terrorism financing and proliferation financing of weapons of mass destruction or the application of legislative requirements regarding PEPs.

In addition to guidance, in the period under review the FMC also published annual reports and excerpts of the NRA and its key findings.

Weighting and Conclusion

Minor deficiencies remain in relation to the provision of guidelines, in particular to DNFBPs in applying the AML/CFT measures. **Armenia is C with R.34.**

RECOMMENDATION 35 – SANCTIONS

In its 2015 MER, Armenia was rated LC with R.35. There have been some changes to the legislation, particularly in the adoption of criteria on the proportionality of sanctions imposed by administrative bodies and the introduction of new thresholds. The changes are not considered material by Armenian authorities. Accordingly, the below analysis is based on 2015 MER findings, with minor amendments to reflect updated legal references and the newly introduced thresholds.

Criterion 35.1 – Generally, Armenia has a wide range of administrative sanctions available to deal with natural as well as legal persons who fail to comply with the AML/CFT Law. There are sanctions available to cover all relevant obligations regarding R.6 and 8 to 23.

In case of infringements of the AML/CFT Law by FIs the relevant sanctions of the sector specific laws apply (AML/CFT Law, Art. 30(2)). If a sector specific law does not provide any responsibility measures for non-compliance with the AML/CFT Law, the sanction measures of the AML/CFT Law apply (AML/CFT Law Art.30(3)). All FIs sectoral regulations include relevant sanctions for violations of AML/CFT regulations, except for pawnshops (Bank and Banking Law, Art 60 and 61; Law on Credit Organisations, Art. 18 and 19; Currency Regulation Control Law, Art. 10; Insurance Law, Art. 143; Investment Fund Law, Art. 106; PSSPO Law, Art. 26; Securities Law, Art. 209). For pawnshops, the sanctions of the AML/CFT Law apply.

If DNFBPs breach AML/CFT obligations, the AML/CFT Law applies directly to legal persons. With regard to DNFBPs that are natural persons, there are sanctions available under the Code of Administrative Offences (Art. 165.9 of the Code of Administrative Offences and Art. 30(4) of the AML/CFT Law).

Each supervisory body (respectively the CBA for FIs) is responsible to sanction infringements of their supervised entities (AML/CFT Law, Art. 29(1) and CBA Law, Art. 39^{1},39^{8} and 39^{9}; Games of chance and Casinos Law, Art. 9(1), Lotteries Law, Art. 10(1)).

Dissuasive: the full range of sanctions for financial institutions appears to be dissuasive. For AML/CFT failures of banks, credit organisations, insurance companies, insurance intermediaries, investment companies, investment funds, pension fund managers, PSOs and pawnshops, the CBA can apply the following sanctions: warnings and directives or remedial sanctions to eliminate infringements; fines; deprivation of bank managers' qualification certificate and nullification of the licence.

The revocation of a banking licence, a licence under the Insurance Act or a licence of credit organisations has to be published. The CBA may also publish sanctions imposed on pension fund managers.

The amount of a fine for banks for a single violation of a requirement other than prudential requirements, including AML/CFT violations, shall not exceed one percent of the amount of the minimal statutory fund (Law on Banks and Banking, Art. 63(3)). The size of the statutory fund of a bank shall be set by its charter and amount at least AMD 1 billion (approximately EUR 2.5 million). (Regulation 2 On the "Regulation of Banking, Prudential Requirements for Banking", Clause 15). The minimum amount for each violation of a requirement other than prudential is AMD 10 million (approximately EUR 24 000). The maximum recorded amount was AMD 90 million (approximately EUR 218 000) for several violations of the AML/CFT Law.

The amount of fines imposed for each violation of insurance companies and insurance intermediaries shall not exceed the 2 500-fold of the minimum salary (approximately EUR 4 500)[115] (Insurance Law, Art. 147). For investment companies, investment funds, pension fund managers the maximum shall not exceed the 2 000-fold of the minimum salary (approximately EUR 3 600); and for PSOs – the 500-fold of the minimum salary (approximately EUR 900) (Securities Law, Art. 211, Investment Funds Law Art. 108). For pawnshops, the maximum amount is AMD 500 thousand (approximately EUR 900) (Article 165.9 of the Code of Administrative Offences and Article 30(4) of the AML/CFT Law).

For failures of money exchange offices, the CBA can issue warnings, impose penalties/fines and suspend/or withdraw the licence (Currency Regulation Control Law, Art. 10). For PSOs, the CBA has the following sanctioning powers: give warnings and charge the institution to eliminate infringements; prohibit the activity of a PSO or in case of a foreign PSS withdraw its authorisation; demand a change of management of the Armenian PSO or terminate or withdraw its authorisation or impose fines (Law on PSSPO, Art. 15 and 27) (see also the analysis for c.27.4). However, the decision to impose a sanction can be waived by the CBA if the FI or its manager resolves the breach prior of the adoption of the decision of imposition (CBA Law, Art. 39[12], point 2).

Proportionate: The Security Market Law, the Insurance Act, the Law on Funded Pensions, the Currency Control Act, and the Law on Pawnshops as well as the Law on Investment Funds define in detail which elements the CBA has to take into consideration while imposing a fine (e.g. nature of the violation, existence of damage, extent of the unjustified enrichment etc.). The Banking Act does not define details which should be taken into consideration while imposing a fine on a bank. However, there is a manual concerning the procedure for the imposition of sanctioning measures in place, which describes the processes and procedures to make fining decisions which also applies to banks including the circumstances and factors considered in the context of the selection of sanctioning measures. This manual includes a list of factors, both aggravating and mitigating, to be taken into consideration, but it does not prescribe any specific formulas or quantitative indicators, leaving the final calculation to be based on professional judgement.

With regard to DNFBPs, only the following sanctions are available: warnings, fines and assignments for eliminating the violation. The prescribed amounts of fines for legal persons DNFBPs for breaches of the AML/CFT Law varies between 500-fold to 5 000-fold the minimum salary (approximately EUR 1 100 – EUR 11 000), which is rather limited in case of some more material DNFBPs (Article 30(4) of the AML/CFT Law). For failure to freeze property of designated persons, the amount of the fine varies between 1 000-fold to 10 000-fold the minimum salary (EUR 2 200 – EUR 22 000). For DNFBPs that are natural persons the amount of the fine for AML/CFT breaches varies between 100-fold minimum salary and 300-fold the minimum salary, with the exception of the failure to freeze property of designated persons, when the fine is in the amount of 1 000-fold the minimum salary (AML/CFT Law, Art. 30(5); AO Code, Art. 169.5).

115. The minimum salary (calculation base for fines, penalties etc.) at the moment of the on-site visit was AMD 1 000 (approximately EUR 1.8).

Referring to the NRA, the average monthly salary in Armenia is AMD 146 524 (EUR 265) and the average monthly salary of a compliance officer of a financial institution, for example, is approximately EUR 1 000. Infringements of AML/CFT requirements by natural persons shall be examined by the relevant supervisory body respectively the authorised body, on behalf of which, the head of the respective supervisory body shall impose administrative sanctions (AO Code, Art. 244.12).

Criterion 35.2 – In case of FIs, apart from the Law on Pawnshops, all other sector specific laws of FIs provide the CBA with the power to sanction the supervised entity as well as their directors respectively the management.

Managers of banks, for example, are the chairman of the board, his deputy, members of the board, executive director, chief accountant, head of internal audit, members of the internal audit, members of banks directorate, as well as heads of territorial and structural subdivisions of the bank, as well as employees of the departments having in the well-reasoned opinion of the CBA a direct link to the main activities of the bank, or having any influence on decision-making process. For any infringements of the law, the CBA may apply to the bank and/or the bank's management (except for members of the board) both, the warning with the order to eliminate the infringements and/or penalise the bank or the bank's manager, and/or deprive the bank managers of the qualification certificates. (Banks and Banking Law, Art. 63(5) and Art. 64, Insurance Law, Art. 147(4) and 148; Investment Funds Law, Art. 108(2) and 108(5), Art. 109, Securities Law, Art. 211(3.1), 211(3.2), 211(3.3) and 213; PSSPSO Law, Art.27(1), 27(4), 27(6); Currency Regulation Control Law, Art. 71; Credit Organisations Law, Art. 19(2), 19(4)). Supervised insurance companies and insurance intermediaries, pension fund managers and fund management companies as well as their managers may be subject to all sanctions available under their sector specific laws. For infringements of laws the CBA may impose a penalty on PSOs or its managers or withdraw the certificate of qualification for managers of PSOs. There is no explicit legal basis to sanction directors and senior management of pawnshops.

There is no legal basis to sanction directors or the senior management of other DNFBPs.

Weighting and conclusions

The range of sanctions available to the supervisor of FIs is broad and includes dissuasive measures such as termination of license or suspension of activity. While the legal framework allows certain breaches to remain unsanctioned if remedied promptly, and although the determination of the final sanctions relies partly on supervisory judgement, overall, the sanctions are proportionate and dissuasive. For DNFBPs, the range of sanctions is more limited, and monetary penalties are less dissuasive, particularly for more material entities such as casinos; however, given the lower materiality of most DNFBP sectors in Armenia's context, these shortcomings carry limited weight. **Armenia is LC with R.35**.

RECOMMENDATION 36 – INTERNATIONAL INSTRUMENTS[116]

In its 2015 MER, Armenia was rated LC with R.36, based on the fact that the country has not acceded to 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft and 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation. R.36 did not undergo a follow-up review. Since then, Armenia adopted in 2024 a new law on legal assistance in criminal proceedings (LACP Law), which is in line with the requirements of the Palermo Convention, the Merida Convention and the Terrorist Financing Convention. Since the last MER, the Court of Cassation's interpretation of the legal provisions related to the ML offence (as issued in 2018, 2019, and 2021) has narrowed the scope of certain ML acts defined under the Vienna and Palermo Conventions. These developments are considered material. On this basis, R.36 is regarded as a

116. The UNCAC Implementation Review Mechanism (IRM), for which the UNODC serves as secretariat, is responsible for assessing the implementation of the UNCAC. The FATF assesses compliance with FATF Recommendation 36 which, in relation to the UNCAC, has a narrower scope and focus. In some cases, the findings may differ due to differences in the FATF and the IRM's respective methodologies, objectives and scope of the standards.

recommendation under review (RUR).

Criterion 36.1 – Armenia is a party to the Vienna Convention, the Palermo Convention, the Merida Convention, and the Terrorist Financing Convention. It should be noted that it has become a party to, *inter alia*, the 2005 Warsaw Convention of the Council of Europe.

Criterion 36.2 – This criterion requires the full implementation of a range of specified articles of the UN Conventions mentioned above. However, in accordance with the interpretation of the legal framework in Armenia by the Court of Cassation decisions (EKD/0090/01/09) the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime, requires an additional element to be considered as money laundering (see R.3). This implies the scope of the aforementioned offences is narrower than as defined in the Vienna and Palermo Conventions (Vienna Convention, Art. 3(1)(c)(i), Palermo Convention, Art. 6(1)(b)(i)). Armenia has not ratified the 2005 Protocol to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf. This means that acts within the scope of this treaty are not covered by the TF offence as required by article 2(1)(a) of the Terrorist Financing Convention (see R.5).

Weighting and Conclusion

Shortcomings remain. Not all elements of the ML offence defined in the Vienna and Palermo conventions are applicable in Armenia. The scope of the TF offence does not cover the acts under the 2005 Protocol to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, as required by the Terrorist Financing Convention. **Armenia is PC with R.36.**

RECOMMENDATION 37 - MUTUAL LEGAL ASSISTANCE

In its 2015 MER, Armenia was rated LC with R.37, based on the following deficiencies: no legislative provision to address the issue of prioritisation of requests; no case management system within the GPO; the reservation to Article 2 of the Protocol permitting to refuse assistance on the grounds involving fiscal matters; the reservation to Article 2 of the Convention permitting refusal of assistance on the grounds of absence of dual criminality even of non-coercive types; the reservation to Article 5 of the Convention allowing the application of dual criminality requirement to requests involving search and seizure. Since then, Armenia has adopted the Law on legal assistance in criminal matters in 2024. The changes are not considered material in the context of R.37 as the new law reflects the framework previously included in the CPC and thus, the below analysis represents the 2015 MER findings.

Criterion 37.1 – The LACP Law allows for the provision of mutual legal assistance in criminal matters on the basis of bilateral or multilateral agreements. Armenia has concluded several bilateral treaties of this kind and is a party to a range of relevant multilateral treaties, including the European Convention on Mutual Assistance in Criminal Matters of 1959. The LACP Law also permits the provision of assistance on an ad hoc basis. Furthermore, the Armenian authorities may utilise any powers provided for in the aforementioned act on behalf of a third country that could be taken with respect to a domestic investigation or prosecution (Article 9 of the LACP Law). It thus possesses a legal basis that allows it to provide a wide range of assistance in relation to investigations, prosecutions and related proceedings involving ML, TF and associated predicate offences.

Criterion 37.2 – The LACP Law contains relevant provisions which regulate the transmission and execution of requests for MLA (Articles 7, 9 and 19 of the aforementioned act). There is no legislative provision which addresses the issue of prioritisation of requests and the evaluators are not aware of an established process in this respect. However, they were assured that within the MoJ in instances of extreme urgency and when so requested a case would be prioritised internally. The MoJ possesses both manual and electronic case management systems to monitor the progress of requests. It is understood that there is no case management system within the GPO.

Criterion 37.3 – Article 19 of the LACP Law stipulates that requests for assistance (in the absence of international treaties) shall not be executed if execution may harm the constitutional order, sovereignty, security or public order of the Republic of Armenia, or put other overriding interests of the Republic of Armenia at risk (see also, Article 11 of the aforementioned act). Though framed in mandatory terms these grounds for refusal of assistance are common in international practice and are not regarded by the evaluators as unreasonable or unduly restrictive.

Criterion 37.4 – The refusal of assistance on the sole ground that the offence is also considered to involve fiscal matters is not provided for in the LACP Law. Furthermore, Armenia is a party to the 1978 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Article 1 of the Protocol explicitly removes this ground for refusal of assistance. However, in its reservation of 23 March 2004 to Article 2 of the Protocol Armenia has indicated that "it will not make the execution of letters rogatory for search and seizure" in this context (see further the discussion of dual criminality in 37.6 below). This presents a point of tension with the requirements of Criterion 37.4(a). Legal and professional privilege and secrecy are not grounds for refusal for mutual legal assistance.

Criterion 37.5 – It is common for relevant international agreements to which Armenia is a party to contain specific provisions requiring the confidentiality of MLA requests to be maintained and these have force in Armenian law by virtue of Article 9 of the LACP Law). In other circumstances the Armenian authorities are of the view that Article 186 of the CPC forms the basis for the necessary protection.

Criterion 37.6 and 37.7 – Unlike in the context of extradition, Armenian law does not generally require the satisfaction of dual criminality for mutual legal assistance. It is not listed as a mandatory ground of refusal in the Law (see above). Article 90 of the LACP Law permits but does not require the refusal of recognition of a foreign court judgment on this basis. Notwithstanding the absence of a stipulated general provision on dual criminality, the 5th round mutual evaluation did not find out any facts or evidence on-site, suggesting dual criminality is required.

Where a request is based on a pre-existing treaty, the grounds for refusal contained in it govern the situation (see, e.g., Articles 11 and 90 of the LACP Law). It should be noted that on 25 January 2002 Armenia made a reservation to Article 2 of the 1959 European Convention on Mutual Assistance in Criminal Matters to permit it to refuse assistance on the grounds of absence of dual criminality even of non-coercive types. This stance sits uneasily with the expectations articulated in Criterion 37.6. A reservation of the same date to Article 5 triggered a dual criminality requirement in respect of letters rogatory for a search and seizure.

The above posture in respect of dual criminality in case of fiscal crime and not involving coercive action (search and seizure of property) has negative implications for co-operation and also in areas where there are technical shortcomings such as the absence of criminal liability for legal persons.

As explained further in the analysis of R.39 on extradition below, the concept of dual criminality in the CPC is such as to satisfy the requirement of Criterion 37.7.

Criterion 37.8 – All the required investigative techniques that are available under domestic law are also available for the purpose of mutual legal assistance except for the exemptions provided by the relevant treaties.

Weighting and Conclusion

Minor shortcomings remain under R37: no legislative provision to address the issue of prioritisation of requests; no case management system within the GPO; in its reservation of 23 March 2004 to Article 2 of the Protocol Armenia has indicated that "it will not make the execution of letters rogatory for search and seizure” on the ground that the offence is also considered to involve fiscal matters; Armenia made a reservation to Article 2 of the 1959 European Convention on Mutual Assistance in Criminal Matters to permit it to refuse assistance on the grounds of absence of dual criminality even of non-coercive types. A reservation to Article 5 triggered a dual criminality requirement in respect of letters rogatory for a search and seizure. **Armenia is LC with R.37.**

RECOMMENDATION 38 – MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION

In its 2015 MER, Armenia was rated LC with R.38. This was mainly due to the lack of formal arrangements for co-ordinating seizure and confiscation actions with other countries, as well as of measures enabling the recognition of civil forfeiture orders under any circumstances. R.38 did not undergo a follow-up review. The FATF Standards for R.38 have undergone a revision against which the country has not previously been assessed. On this basis, R.38 is regarded as a recommendation under review (RUR).

Criterion 38.1 – The provision of MLA concerning seizure and confiscation is undertaken on the basis of the legislation regulation legal assistance in criminal proceedings, which includes the Constitution, the LAPC Law, the Criminal and Criminal Procedure Codes, the Penitentiary Code and internation treaties ratified by the country (LAPC Law, Art. 2(1)). The country is a Party to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism Warsaw Convention which contains provisions for mutual legal assistance in relation to freezing and confiscation (Articles 21–23). To assist with requests aimed to identify, trace, evaluate, investigate criminal property and property of corresponding value, the same investigative powers established by the CPC are available (LAPC Law, Art. 1(2)). These are subject to the same requirements. The limitations described under R.30 and R.31 may impact both the scope and the timeliness of assistance, particularly in relation to access all necessary information to support the identification and tracing of criminal property and property of corresponding value (see R. 30, 31 c.31.1(a) and 31.3 (a)).

Criterion 38.2 – Recognition and enforcement of foreign freezing, seizing and confiscation orders and convictions is governed under the international treaties (see R.36). In the absence of such, the LACP Law also envisages a mechanism for providing assistance (Articles 19-20). The recognition and enforcement orders made on the basis of non-conviction-based confiscation shall be executed based on reciprocity in the area of mutual assistance, unless the execution thereof does not contradict the public order of the Republic of Armenia. (Article 29, CFLA Law).

Criterion 38.3 – There are no legal provisions requiring Armenian authorities to conduct a domestic investigation prior to the execution of foreign orders concerning freezing, seizing, and confiscation. The judiciary plays a supervisory role in ensuring compliance with Armenian law, but there is no requirement to re-assess the facts indicated in a request, as long as the foreign order complies with Armenia’s international obligations or is based on the principle of reciprocity.

Criterion 38.4 – While there are no explicit provisions requiring that when the requested country requires a court order to provide assistance due to fundamental principles of domestic law or other considerations, articles 133 of the CPC on attachment of property for seizure, and 121 of the CC on confiscation ensure that Armenian courts have the authority to issue freezing, seizing and confiscation orders for property located abroad.

Criterion 38.5 – As outlined in Recommendation 4, the management of the seized property during the pre-trial stage, as well as of the confiscated property falls under the responsibility of multiple agencies, depending on the nature of the seized or confiscated property (see c.4.11). The deficiencies regarding the lack of systematic management framework impacts the compliance with this c.

Criterion 38.6 – The Deputy Head of the General Criminal Police Department of the MIA, who is also the Head of the Interpol NCB in Armenia along with the GPO are the contact points for the Camden Asset Recovery Inter-Agency Network (CARIN). By co-operating with the contact points of the specified network in other countries, it is possible to receive requests from the latter, carry out background checks and send the information received in the same way. No limitations were identified, which would prohibit authorities to provide information based on the initial request.

Criterion 38.7 – Sharing property with foreign states requesting assistance is governed by Article 93 (6 & 7) of LACP Law. In accordance with these provisions, priority is given to compensation of damage caused to victims and return of property to rightful owners, which should be carried out by the requesting state. From the remaining assets - half of the confiscated assets or half of their value shall be transferred to the requesting party. Article 93 (7) explicitly indicates that Armenia may conclude agreements implementing alternative rules for distribution of property with interested foreign states of general nature or concerning individual cases, allowing to deduct or share substantial or extraordinary costs incurred when enforcing a freezing, seizing, or confiscation order.

Criterion 38.8 – As indicated under 38.1 Armenian authorities have a broad set of legal powers to address legal assistance. The Country has ratified various international treaties and conventions that promote co-operation in asset recovery. This includes agreements under the United Nations and Council of Europe conventions, such as the UN Convention against Corruption (UNCAC), UN Convention on Transnational Organized Crime (UNTOC), the Warsaw Convention, and the European Convention on Mutual Assistance in Criminal Matters. No further information was provided on additional mechanisms such as bilateral agreements and examples of regional co-operation mechanisms that allow the country to work effectively with foreign nations in the identification, freezing, seizure, and confiscation of illicit property.

Weighting and Conclusion

All the criteria are either met or mostly met. The remaining shortcomings include: the limitations of the powers to access financial information may impact both the scope and the timeliness of assistance for identification and tracing criminal property (c.38.1); the lack of systematic management of seized and confiscated property as described under R.4 (c.38.5); and no alternative mechanisms to enhance co-operation in asset recovery (c.38.8). **Armenia is LC with R.38.**

RECOMMENDATION 39 – EXTRADITION

In its 2015 MER, Armenia was rated as LC with R.39, based on the fact that there were no simplified procedures for extradition. Since then, Armenia has adopted the Law on legal assistance in criminal matters in 2024. The changes are not considered material in the context of R.39 and thus, the below analysis represents the 2015 MER findings.

Criterion 39.1 – Armenia is able to provide extradition based on bilateral or multilateral agreements and it has become a party to the European Convention on Extradition of 1957 and to the 1st and 2nd Protocols thereto. Under the LACP Law can also take place on an ad hoc basis (see, e.g., Articles 28—38, 56-62). Both ML and TF are extraditable offences.

Armenian law (primarily the LACP Law) contains clear provisions on the execution of extradition requests. There are both manual and electronic case management systems in the MoJ which are relevant in this context. While the law does not address prioritisation of requests the evaluators were assured that in cases of urgency priority would be afforded to the request internally on an ad hoc basis.

Armenian law does not place unreasonable or unduly restrictive conditions on the execution of extradition requests (see, e.g., Article 33(2) of the LACP Law).

Criterion 39.2 – Article 55.2 of the Constitution of the Republic of Armenia (2015) states that citizens may not be extradited "with the exception of cases stipulated in international treaties" to which it is a party (see also Article 33(point 3 of part 2 of the LACP Law)). However, Armenia has never concluded a treaty permitting the extradition of citizens. In instances, inter alia, where extradition is declined on the grounds of nationality the individual in question, upon the request of the foreign state, must be prosecuted domestically (Article 173(5) of the CPC; see also Article 15(1) of the CC).

Criterion 39.3 – The LACP Law does not directly provide a regulation on dual criminality, however such approach is based on international treaties and provides references thereto. Armenia is party to the European Convention on Extradition, the European Convention on the Transfer of Sentenced Persons, the UN Convention on Transnational Organized Crime, the UN Convention against Cybercrime, the Minsk Convention and the Chișinău Convention.

Criterion 39.4 – R.39, as revised by the FATF in 2012, requires countries (subject to consistency with fundamental principles of domestic law) to have simplified extradition mechanisms in place. The Armenian authorities have confirmed that there are, at the present time, no such simplified procedures for extradition. The authorities did not indicate that Armenia intended to sign the Third Additional Protocol to the European Convention on Extradition (CETS 209).

Weighting and Conclusion

Minor shortcomings remain with regard to the lack of simplified procedures for extradition. **Armenia is LC with R.39.**

RECOMMENDATION 40 – OTHER FORMS OF INTERNATIONAL COOPERATION

In its 2015 MER, Armenia was rated C with R.40. The FATF Standards for R.40 have undergone a revision against which the country has not previously been assessed. On this basis, R.40 is regarded as a recommendation under review (RUR).

General Principles

Criterion 40.1 – A general provision under the Armenian AML/CFT Law grants the competent bodies with the authority to co-operate with international structures and other relevant bodies of foreign countries, in the field of combating ML and TF (Article 14(1) of the AML/CFT Law). The wording is wide enough for compliance with Criterion 40.1 in respect of all competent authorities combatting money laundering and terrorism financing.

FMC

For the FMC there is an express authority to exchange information (including documents and classified information) spontaneously and on request, as defined by the law, with foreign financial intelligence bodies, which, based on bilateral agreements or commitments due to membership in international structures, ensure an adequate level of confidentiality of the information and use it exclusively for the purposes of combating money laundering and terrorism financing (Article 10(1) 17 and Article 14(2) of the AML/CFT Law). This authority extends also to indirect (via foreign FIU) exchange of information with foreign supervision authorities competent in the field of combating ML/FT, for supervision purposes (Article 14(1) of the AML/CFT Law).

LEAs

Co-operation in combating money laundering and terrorism financing with international structures and relevant bodies of foreign countries Is conducted within the framework of international treaties or, in the absence of such treaties, in accordance with international practice. The basic principles ensuring confidentiality of the information, not disclosing this information to any third party and using it exclusively for the purposes of combating money laundering and terrorism financing, are regulated under Article 14 of the AML/CFT Law. At the same time, regulations with regard to co-operation (interaction) with foreign special services and law enforcement bodies in the area of operational intelligence activity in general are envisaged under Point 15 of Paragraph 1 of Article 15 and Article 18 of the National Security Bodies Law as well as under Point 2 of Paragraph 1 of Article 11 of the OIA Law.

SUPERVISORS

Financial institutions

The Central Bank of Armenia is authorised to co-operate with foreign financial supervision bodies in the framework of bilateral and multilateral agreements, which regulate matters related to the exchange, use, and dissemination of confidential information on on-site inspections and off-site supervision, regulatory, prudential and other information. Based on such agreements, foreign supervisory bodies are also allowed to conduct on-site inspections in Armenia resident branches and other establishments of the financial groups headquartered abroad (Articles 8(1) & art 39^1(1) of the Law on CBA). Information may be provided both spontaneously or upon request.

DNFBPs

The Ministry of Justice is authorised to co-operate with their respective foreign counterparts in accordance with the provisions of the Law on International Treaties. In particular, it is empowered to sign interagency treaties with foreign supervision bodies in order to facilitate effective co-operation on the matters of mutual interest (Articles 6(5) and 7(4) of the Law on International Treaties). More specifically, the ministry is authorised to co-operate with their foreign counterparts on the matters related to supervision of relevant DNFBPs, including compliance of the DNFBPs with the AML/CFT requirements (Article 14(1) of the AML/CFT Law). There are two separate departments dealing with cooperation, the Mutual legal Assistance Department and the International Legal Cooperation department of the MOJ, which facilitate international co-operation of the ministry within the framework of their powers and mandate. Article 14(1) of the AML/CFT Law also applies to international cooperation of the SRC in its supervisory function.

Criterion 40.2 –

Competent authorities:

(a) Have a general lawful basis for providing international co-operation (Article 14(1) of the AML/CFT Law). Additionally, FMC, police, national security agencies, tax and customs authorities, have specific texts under their statute laws or other legislation, that allow for such co-operation (Article 14(1 & 2) of the AML/CFT Law; Article 15 (1)(15) of the Law on National Security Agencies*; Article 369 of the EEU Customs Code*, Article 10(2) of the LOIA); authority for CBA in this respect is provided by the Law on CBA (Articles 8(1) & 39^1(1)). The authority of the of the Ministry of Justice is provided by the Law on International Treaties (Articles 6(5) & 7(4));

(b) Have no legal limitation on their authority to use the most efficient means to co-operate.

In accordance with Article 14 (1) of the AML/CFT Law, even in the absence of formalized treaties or bilateral agreements competent authorities tasked with combatting ML/TF are authorized to exchange information in accordance with international practice.

(c) Use clear and secure gateways for the transmission or execution of co-operation requests such as:

FMC – Egmont Secure Web, CIS FIU mail and FMC mail (Clause 54 of the FMC Operational Manual);

Central Bank and Ministry of Justice – channels agreed by the bilateral agreements concluded with foreign counterparts;

LEAs – different (including electronic) secure channels e.g. Interpol network, Customs Enforcement Network.

(d) The FMC has clear processes for the prioritisation and timely execution of co-operation requests (Clauses 55-59 of the FMC Operational Manual). The process of prioritisation of incoming signals (including international requests) by the FMC is detailed in the *STR Prioritisation Rules*. According to the authorities, LEAs execute requests pursuant to the timeframes indicated by the foreign counterparts, spreading from 10 days to 3 months, depending on the nature and other circumstances of the request. Also, CBA abides by the bilateral agreement provisions it has concluded with foreign counterparts. The Ministry of Justice is bound by the provisions of respective interagency agreements. The SRC has written procedures governing the prioritisation process.

(e) The FMC has clear processes for safeguarding information received (AML/CFT Law Article 14(3) and (Clauses 55-59 of the FMC Operational Manual). According to authorities, any information exchanged by LEAs with foreign counterparts is rated as confidential and it is secured according to the concluded bilateral and multilateral agreements and LEA's internal procedures for dealing with such information. As for the CBA, information received from foreign supervision authorities is covered by the provisions of the Banking Secrecy Law. The Ministry of Justice has clear processes to ensure confidentiality of information received from foreign counterparts. Nevertheless, the relevant legislation was not provided to the AT to verify this.

Criterion 40.3 – There are no legal texts that would limit the authority for international co-operation of the competent authorities to bilateral or multilateral agreements only. The wording of Article 14 (1) of the AML/CFT Law makes reference to international treaties or international practice, which excludes such an interpretation.

Criterion 40.4 – Based on the legislation provided, there are no legal limitations that would prevent competent authorities to provide feedback on the use and usefulness of information obtained through co-operation. Being a member of Egmont Group, the FMC provides such feedback in accordance with Clause 19 of the Egmont Principles for Information Exchange. As regards LEAs and the supervisory bodies (CBA, MoJ) no explicit guidelines or legal provisions regulate this aspect. According to the authorities, provision of feedback is mainly governed by bilateral and multilateral agreements signed with foreign counterparts.

Criterion 40.5 - (a) Armenian legislation does not exclude or prohibit the submission of information in the case of tax matters. Tax offences are considered predicate crimes for ML and as such replies are provided.

(b) According to the authorities, both the FMC and CBA are authorised to exchange information which is subject to secrecy (Article 14(2) of the AML/CFT Law, Articles 8 and 39^1(1) of the Law on CBA). The Ministry of Justice is empowered to exchange confidential information in accordance to the interagency treaties. LEAs do not seem to be limited in exchanging such information with counterparts, although the relevant legislation was not provided to the AT.

(c) According to the authorities, the legislation provided does not exclude or prohibit the submission of information by competent authorities when there is an inquiry, investigation or proceeding underway. Legislation (Article 14(1) of the AML/CFT Law) provides for co-operation with international structures and relevant bodies of foreign countries, making no distinction on the nature or status of such counterparts.

Criterion 40.6 – According to Article 14(3) of the AML/CFT Law, FMC is not authorised to disclose the received information to a third party, as well as to use or share it for criminal, prosecutorial, administrative and juridical purposes without the prior consent of the foreign authority which has provided the information. As regards LEAs, the CBA and the Ministry of Justice, according to the authorities, multilateral and bilateral agreements in force prohibit the use or disclosure by parties of received information, to any third party, without the prior consent of the provider.

Criterion 40.7 – In addition to the provision of Article 14(3) of the AML/CFT Law, the staff of the FMC is under an obligation to maintain confidentiality of classified information both in the course of performing their duties and after termination thereof.

According to authorities, any information exchanged by LEAs with foreign counterparts is rated as confidential and it is secured according to the bilateral and multilateral agreements concluded, to the provisions of the Secrecy Law and LEA's internal procedures for dealing with such information.

Also, confidentiality and non-disclosure of information received from foreign supervisory bodies is guaranteed by the Bank Secrecy Law and provisions of the international agreements concluded by the CBA. All CBA staff members sign an agreement on confidentiality of information. In case of the Ministry of Justice, privacy and data protection regime of information received from the foreign counterparts is regulated by interagency agreements. In addition, non-disclosure of the received information to third parties is ensured by the internal procedures regulating information secrecy regime.

Criterion 40.8 – There is no provision under the AML/CFT Law that would prevent FMC from conducting inquiries on behalf of foreign counterparts. Also, Article 14 of the AML/CFT Law makes no distinction on the information FMC may exchange – obtained or obtainable. At the same time, the FMC has the capacity to request and obtain from reporting entities other information (including documents) for AML/CFT purposes. It is also authorised to request information (including documents) for the same purpose from state bodies, including supervisory bodies and authorities involved in operational intelligence activities, as well as from public participants in proceedings (AML/CFT law Art. 10 (1,4 & 5)).

As regards LEAs, they have the ability to conduct inquiries on behalf of foreign counterparts (Article 10(2) of the LOIA). The LCBA provides that the CBA can co-operate with foreign authorities with supervisory powers disclosing all information that is necessary for them to conduct their supervision, including confidential information. There are no provisions limiting the CBA from requesting such information for the foreign counterparts on their behalf (Article 39^1(1) of the Law on the CBA). Information exchange matters, including obtaining information for and on behalf of foreign counterparts are regulated by interagency treaties of the Ministry of Justice.

Exchange of Information between FIUs

Criterion 40.9 – Article 14 of the AML/CFT Law provides for the FMC an adequate legal basis for co-operation on money laundering, associate predicate offences and terrorist financing. The wording "relevant bodies and foreign financial intelligence bodies" makes no distinction on the legal nature or status of such organisations consequently allowing co-operation. Also, although the text states that co-operation is done with bodies involved in combating ML/TF, the framework for such co-operation – international treaties or international practice – allows for co-operation on associate predicate offences too.

Criterion 40.10 – There is no legal provision that would prevent the FMC to provide feedback to its foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided. Also, being a member of Egmont Group, the FMC provides such feedback in accordance with Clause 19 of the Egmont Principles for Information Exchange.

Criterion 40.11 – The wording of Article 14 of the AML/CFT Law or the FMC Operational Manual place no limitations on the categories of information that could be exchanged by the FMC with foreign counterparts. Membership of the FMC in the Egmont Group enables the exchange of relevant information in accordance with provisions of Clause 22 of the Egmont Principles for Information Exchange. Thus, there is no legal impediment that would prevent the FMC from exchanging the categories of information mentioned by Criterion 40.11.

Criterion 40.12 – In accordance with Article 26 (2) of the AML/CFT Law, the FMC is authorised to immediately suspend the transaction or business relationship for a period of up to 15 days based on the filed reports, requests from foreign financial intelligence bodies, analysis of information provided by supervisory bodies and authorities involved in operational intelligence activities, as well as by public participants in proceedings, or of other information. The resolution of the FMC to suspend the transaction or business relationship should be implemented immediately upon receipt thereof by the financial institution. There is no possibility for the FIU to take such measures in the case of DNFBPs.

In accordance with Article 14(1) of the AML/CFT Law, the FIU can also cooperate directly and indirectly with non-counterparts (i.e. diagonally) dedicated to combatting ML/FT. which in practice includes requests sent by the FMC to counterparts concerning the suspension of transactions.

Exchange of information between financial supervisors

Criterion 40.13 – CBA has the legal basis for providing co-operation to foreign counterparts and may exchange supervisory information relevant for AML/CFT purposes (CBA Law, Articles 8(1) and $39^1(1)$).

Criterion 40.14 – The legislation does not limit the authority of CBA to exchange with foreign counterparts the information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs.

Criterion 40.15 – Article 39(1) of the Law on CBA empowers CBA to transfer all lawfully possessed information to other supervisors that have a shared responsibility for FIs operating in the same group. The provision is wide enough to cover the categories of information (regulatory, prudential and AML/CFT) provided by Essential Criterion 40.15.

Criterion 40.16 – The LCBA provides general regulation of international co-operation between the CBA and foreign counterparts, whereas details on the specific ways of co-operation are provided by international or bilateral agreements signed by the CBA. For example, in line with the MoUs signed by the CBA, these regulate *inter alia* co-operation with foreign counterparts on matters related to establishment, licensing and on-going supervision of financial organisations founded in Armenia or in the relevant foreign country. This includes the exchange of information based on requests made in writing or, in case of urgency, any other mutually agreed form. Co-operation is also possible in the absence of an official multilateral/bilateral agreement (CBA Law, Art. 8). Hence, there are no limitations for the CBA to proceed with request and conduct any supervisory activity including conducting inquiries on behalf of foreign counterparts whenever requested.

Moreover, based on international or bilateral agreements, foreign supervisory bodies are allowed to conduct on-site inspections in Armenia resident branches and other establishments of the financial groups headquartered abroad (Articles 8(1) & $39^1(1)$ of the Law on CBA). There are no limitations in the legislation for the foreign financial supervisory bodies to conduct inquires themselves in order to facilitate effective supervision of financial groups.

Criterion 40.17 – Supervisory information constitutes classified information (work related secret) (CBA Law, Art. 28)., Apart from that, there is no general requirement in the CBA Law for the central bank to use or disseminate the information received from a foreign counterpart only on the basis of a prior authorisation or to inform their foreign counterpart of any legally mandatory obligations to disclose or report the received information. Nevertheless, detailed regulation of international co-operation is provided under the multilateral or bilateral agreements (MoUs) signed by the CBA. For example, when exchanging information, CBA shall ensure confidentiality of received information, use exclusively for lawful supervisory purposes, and refrain from disclosing the received information without a prior consent of the foreign counterpart. In case the CBA is legally compelled to produce information, it shall endeavour to ensure confidentiality of received information and promptly consult with foreign counterpart. Specifically, CBA shall not be authorised to disclose to any third party the AML/CFT related information received within the framework of international co-operation, as well as to use it or share it for criminal prosecution, administrative or judicial purposes, without the prior consent of the foreign institution that provided such information. (AML Law, Art. 14(3)). However, no such requirement exists for information exchanged for prudential purposes.

Exchange of information between law enforcement authorities

Criterion 40.18 – Domestically available information (including banking information) may be collected by LEAs either through operational intelligence measures based on LOIA (Article 14 (1) and 15), or through investigatory measures conducted under the CPC. However, the deficiencies identified under R.31 apply. The first category may be disseminated (exchanged) with foreign counterparts based on the provisions of Article 10 (2) of the LOIA. For the second, the authority to exchange it with foreign LEAs should be based on the general co-operation rule provided by the AML/CFT Law (Article 14(1)).

Criterion 40.19 – (a) LEAs are able to exchange domestically available information for intelligence or investigative purposes and co-operate with foreign counterparts to identify and trace criminal property and property of corresponding value, and in support of the freezing, seizing, and confiscation of such property through the formal mutual legal assistance process (LOIA, Article (10(2)), AML/CFT Law, Article 14(1)) (see c.40.18).

(b) The requests initiated by foreign competent authorities for execution in the territory of the Republic of Armenia, are carried out in accordance with the procedures provided for by the international treaties ratified by the Republic of Armenia. In the absence of such treaties, assistance is rendered based on reciprocity, according to arrangements reached through diplomatic channels between the competent authorities of the Republic of Armenia and the foreign state.

Criterion 40.20 – The country sees no limitations on spontaneous sharing of relevant information. although no supporting information on this was provided. The legal framework does not provide explicit provisions for spontaneous dissemination of information.

There appears to be no restrictions for the LEAs to spontaneously identify and trace criminal property and property of corresponding value, in appropriate cases, if they suspect that such property relating to a foreign investigation may be located in their jurisdiction. However, in the absence of explicit legal provisions, the country did not provide examples that would demonstrate this.

Criterion 40.21 – Article 10(2) of the LOIA allows LEAs to carry out operational intelligence measures based on inquiries from law enforcement authorities and special services of foreign countries and international law enforcement organisations, in accordance with international treaties. Nevertheless, the limitations on the scope of the operational intelligence measures may impact the ability of the LEAs to use these powers (see R.31).

Criterion 40.22 – Article 18 of the LACP Law provides for the possibility to establish joint investigative teams within the framework of legal assistance, subject to a special agreement.

Criterion 40.23 – (a) Armenia is a member of Interpol (since 1992) and extensively co-operates with foreign counterparts based on multilateral agreements in the context of Interpol. With Europol, Armenia has signed in 2021 a strategic co-operation agreement for combating cross-border criminal activities. The agreement allows for exchange of general strategic intelligence, as well as strategic and technical information and operational information with the exception of personal data.

(b) Since November 2020, Armenia is a member of the CARIN international operational information network. Two contact points have been designated: one from the GPO and one from the MIA (Head of NCB of Interpol).

All mentioned multilateral networks facilitate international co-operation in asset recovery.

Exchange of information between non-counterparts

Criterion 40.24 – The general co-operation rule provided by Article 14 of the AML/CFT Law allows for co-operation with international structures and relevant bodies of foreign countries (including foreign financial intelligence bodies) involved in AML/CFT within the framework of international treaties or, in the absence of such treaties, in accordance with international practice. This rule does not restrict indirect exchange of information by LEAs or FMC. There is no information on provisions explicitly referring to indirect information exchange between AML/CFT supervisors.

Weighting and Conclusion

Armenia can provide a wide range of international co-operation and meets or mostly meets all the criteria of the recommendation. Minor shortcomings remain. **Armenia is LC with R. 40.**

Annex B. Technical Compliance shortcomings

Annex Table 1. Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	LC	Minor shortcomings remain: • Certain qualitative and quantitative criteria for monitoring progress under the AML/CFT/CPF Strategy and Action Plan remain overly general, and there is a need for clearer prioritisation of actions implementing the Anti-Corruption Strategy for 2023-2026 (c.1.6); • No explicit legal requirement to apply EDD measures in relation to newly identified higher risk scenarios and no requirement to incorporate the identified higher risks into the institutional risk assessment (c.1.8); • The low-risk scenarios are not deriving from the NRA (c.1.9); • No examples of enhanced measures to be applied in case of higher PF risks are provided by the legal framework (c.1.15(d)).
2. National cooperation and coordination	LC	• The legal framework governing the operational cooperation between the FMC and LEAs does not explicitly extend to PF-related matters, and no formal typologies or intelligence sharing mechanisms are in place to ensure systemic operational information exchange between LEAs and intelligence bodies (c.2.4).
3. Money laundering offences	PC	• Not all elements of the ML offence as defined in the Vienna and Palermo conventions are applicable in Armenia (c.3.1); • There is a limited scope of corporate criminal liability (c.3.10).
4. Confiscation and provisional measures	PC	• Uncertainty regarding the policy decisions or documents prioritising asset recovery, and insufficient information on the operational frameworks of all competent authorities with competence in asset recovery (c.4.1(a)); • The actions aimed at providing adequate resources to LEAs have not yet been fully implemented (c.4.1(c)); • Deficiencies identified under R.31 apply, including limitations of the powers to access banking and related information, in the scope of the available investigative techniques, and in timely access to a wide range of information for the identification and tracing of criminal property and property of corresponding value (c.4.2); • The FMC's power to suspend a transaction or business relations cannot be applied on the basis of information received from DNFBPs (c.4.3(a)); • The value threshold for illicit assets applicable to civil forfeiture under c.4.8 and 4.9 has a restrictive impact (c.4.4(c)); • Insufficient information on the measures in place to prevent or void actions that may prejudice the ability to seize or confiscate criminal property or property of corresponding value (c.4.6); • Extended confiscation and civil forfeiture are subject to restrictive condition related to the high value threshold for illicit assets (c.4.8 and c.4.9); • Insufficient information on the framework and mechanisms for cooperation and information sharing between competent authorities and tax authority (c.4.10); • Deficiencies in legal and institutional framework for managing seized and confiscated property (c.4.11).
5. Terrorist financing offence	LC	• Minor gap in the scope of the TF offence (c.5.1) • There is a limited scope of corporate criminal liability (c.5.8).
6. Targeted financial sanctions related to terrorism & TF	LC	• There is no provision which prohibits Armenian nationals or persons or entities within Armenia (other than reporting entities) from making any funds or other assets available to designated persons (c.6.5)
7. Targeted financial sanctions related to proliferation	LC	• Supervisory authorities do not have powers to carry out onsite inspections and review compliance with the requirements PF related TFS obligations (c.7.3)
8. Non-profit organisations	LC	• The steps identified in the AML/CFT/CFP National Strategy to target specific risks within the NPO sector have not yet been fully implemented (c.8.1) • Armenia has not carried out any specific work with the NPO sector to refine and develop best practices (c.8.2) • The measures applicable to NPOs are not fully focused, proportionate and risk based (c.8.3) • The oversight and monitoring of the NPO sector is not fully focused, proportionate and risk based (c.8.4)

Recommendations	Rating	Factor(s) underlying the rating
		• There are no MoUs in place regarding the DRA (c.8.5) • There are limited measures in place for NPOs that are religious organisations
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• The definition of linked transactions is limited to transactions with the same party, having similar nature and occurring within 24 hours (c.10.2) • There is no explicit requirement for FIs to satisfy themselves that they know who the BO is (c.10.5) • There is no explicit requirement for FIs to understand the ownership and control structure of customers that are legal persons (c.10.8) • The law does not expressly require FIs to obtain and document information on the legal form of the legal person/arrangement (c.10.9) • The legal definition does not cover combined ownerships, where two or more natural persons might control jointly a legal person by voting rights or other means (c.10.10) • There is no specific provision for BO identification for situations in which beneficiaries of a trust are designated by characteristics or by class (c.10.11) • SDD measures are not clearly defined and have very limited application (c.10.18)
11. Record keeping	C	
12. Politically exposed persons	LC	• There is no obligation to inform senior management before the payout of the policy proceeds, nor to consider making an STR (c.12.4).
13. Correspondent banking	C	•
14. Money or value transfer services	LC	• Limited dissuasiveness of sanctions for unlicensed activities (c.14.2).
15. New technologies	LC	• ML/TF risks derived from the use of new technologies have been assessed to some extent only (c.15.1) • No comprehensive assessment of overall residual ML/ TF risk for VA or VASPs has been conducted (c.15.3) • CBA's power to reject the application of person that acquires a qualifying holding and has a criminal record is formulated as optional (c.15.4(b)) • Given recent implementation of VASPs licensing, there was no regulatory or procedural framework to ensure the risk-based approach in practice (c.15.6) • There are no further guidelines established for VASPs concerning the application of national measures to combat ML/TF (c.15.7) • Remaining minor deficiencies under R.10-21 apply to VASPs (c.15.9) • Deficiency under c.7.3. applies (c.15.10) • Deficiencies under R.37-40 apply (c.15.11)
16. Wire transfers	C	
17. Reliance on third parties	C	
18. Internal controls and foreign branches and subsidiaries	C	
19. Higher-risk countries	C	
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	LC	• Remaining deficiencies under R.10 and R.15 applicable to DNFBPs (c.22.1 and c.22.4).
23. DNFBPs: Other measures	C	
24. Transparency and beneficial ownership of legal persons	PC	• Deficiencies identified under c.24.3(b) and c.24.10 apply to foreign-created leal persons (c.24.1(d)) • The ML/TF risk assessment of domestic and foreign legal persons is not sufficiently comprehensive (c.24.3) • There are insufficient mitigating measures implemented to ensure timely access to adequate, accurate and up-to-date BO information, both for legal persons registered in Armenia and for foreign legal persons with sufficient links to

Recommendations	Rating	Factor(s) underlying the rating
		Armenia (c.24.3) • There is no requirement to register, record and make public the list of all directors (c.24.4) • Not all legal persons are required to obtain and record the basic information, and while most material legal persons are, this excludes proof of incorporation, status and information on directors (c.24.5(a)) • Partnerships and cooperatives are not required to retain information on their partners or members (c.24.5(b)) • The absence of requirement for legal persons and the Central Depositary to keep shareholder information in Armenia (c.24.5(c)) • Legal persons are not explicitly required to co-operate with FIs/DNFBPs to provide accurate, adequate and up-to-date information on BOs (c.24.6) • No explicit obligation to keep BO information for at least five years after cessation of legal person (c.24.7) • Administrators, liquidators or other persons involved in the dissolution of the company are not obliged to retain records after the legal persons is dissolved or ceased to exist (c.24.7) • The mechanisms ensuring that available BO information is adequate, accurate and up-to-date are not deemed sufficient (c.24.8) • There are certain circumstances when LEAs are not empowered to source basic and BO information from FIs and DNFBPs (c.24.9) • Data on the owners of stock of JSCs must be provided to competent authorities within nine working days which is not deemed timely (c.24.9) • The combination of mechanisms to ensure the availability of BO information for foreign legal persons are not sufficient (c.24.10) • In the case of LLCs, no measures to prevent or mitigate the misuse of nominees are in place (c.24.13) • The sanctioning regime for basic and BO information breaches by legal persons are not deemed effective and dissuasive in view of the extinguishment of liability when breaches are remedied (even when these are serious, systemic, or repetitive breaches), and the statute time limitation to institute proceedings (c.24.14) • Deficiencies identified under R.37 and R.40 apply accordingly (c.24.15).
25. Transparency and beneficial ownership of legal arrangements	PC	• There is no structured analysis on the ML/TF vulnerabilities in relation to legal arrangements, nor an assessment of the effectiveness of controls (c.25.3 (a)(b)) • No analysis of ML/TF vulnerabilities and mitigating measures related to foreign trusts and similar legal arrangements with sufficient links to Armenia (c.25.3(c)) • There is no requirement that the BO information is kept accurate and up-to-date by the trustees and persons managing similar legal arrangements (c.25.6) • No information was provided on whether requests for BO information by AML/CFT supervisors must be complied with in a timely manner (c.25.7(b)) • There is no explicit legal requirement for trustees and persons managing similar legal arrangements to ensure accuracy and that BO information kept is up to date (c.25.8) • There is no explicit legal requirement to identify trust assets (c.25.9) • There is no explicit obligation to hold information on residence of trustees and assets held or managed by the reporting entity (c.25.10) • No information available on sanctions for failing to grant to competent authorities' timely access to information referred to in c.25.4 and 25.5 held by trustee or person holding equivalent position (c.25.11) • Deficiencies identified under R.37 and R.40 apply accordingly (c.25.12)
26. Regulation and supervision of financial institutions	LC	• Deficiencies identified in the Basel Core Principles (c.26.4(a)) • No dedicated assessment of ML/TF risk is performed at the financial group level (c.26.5(c))
27. Powers of supervisors	C	
28. Regulation and supervision of DNFBPs	PC	• No measures to prevent the associates of criminals from holding (or being BO of) a significant or controlling interest of casinos/gambling operators (c.28.1(b)) • The ChoA has limited powers to conduct monitoring of compliance with AML/CFT requirements by advocates (c.28.4(a)) • No measures are in place to prevent criminals or their associates from being professionally accredited or licensed, or holding a significant or controlling interest, being the BO or holding a management function in the DNFBPs supervised by FMC (c.28.4(b)).

Recommendations	Rating	Factor(s) underlying the rating
		• The range of available sanctions for AML/CFT failures of DNFBPs is limited. There is no legal basis to sanction directors or the senior management of DNFBPs (c.28.4(c)) • No risk-based supervision by the SRC and the ChoA (c.28.5)
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	LC	• concerns regarding the timely access to a wide range of information necessary to support the identification and tracing of criminal property and property of corresponding value (c.30.3).
31. Powers of law enforcement and investigative authorities	PC	• The powers to seize banking and similar information are limited in scope (c.31.1(a)); • Limited scope of application of the available investigative techniques (c.31.2); • No timely access in all cases to a wide range of information to support the identification and tracing of criminal property and property of corresponding value (c.31.3(a)).
32. Cash couriers	LC	• Only movements that cross the external borders of the EAEU are subject to the declaration requirements (c.32.1); • Concerns regarding the proportionality of the administrative sanctions for false or non-declaration (c.32.5).
33. Statistics	LC	• No obligation for authorities other than the FIU to maintain statistics on informal information exchange made and received in the course of international co-operation (c.33.1).
34. Guidance and feedback	C	
35. Sanctions	LC	• There is no legal basis to sanction directors and senior management of DNFBPs other than casinos.
36. International instruments	PC	• Not all elements of the ML offence as defined in the Vienna and Palermo Conventions are applicable in Armenia; the scope of the TF offence does not cover the acts under the 2005 Protocol to the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, as required under the Terrorist Financing Convention (c.36.2).
37. Mutual legal assistance	LC	• No legislative provision to address the issue of prioritisation of requests and no case management system within the GPO (c.37.2); • The reservation to Article 2 of the 1978 Protocol to the European Convention on Mutual Assistance in Criminal Matters impacts the compliance with the criterion (c. 37.4); • The reservation to Articles 2 and 5 of the 1959 European Convention on Mutual Assistance in Criminal Matters permits the refusal of assistance on the grounds of absence of dual criminality even in respect of non-coercive types of requests and subjects the execution of rogatory letters for a search and seizure to a dual criminality requirement (c.37.6 and c.37.7).
38. Mutual legal assistance: freezing and confiscation	LC	• Limitations of the powers to access financial information may impact both the scope and the timeliness of assistance for identification and tracing criminal property (c.38.1); • Lack of systematic management of seized and confiscated property as described under R.4 (c.38.5); • No alternative mechanisms to enhance co-operation in asset recovery (c.38.8).
39. Extradition	LC	• There are no simplified procedures for extradition.
40. Other forms of international cooperation	LC	• No underlying information is available to verify the safeguarding and confidentiality requirements applicable to LEAs and supervisory authorities in relation to the received information (c.40.2(e)); • No explicit guidelines or legal provisions regarding the obligation of LEAs and supervisory authorities to provide timely feedback to foreign competent authorities upon request (c.40.4); • The FMC's power to suspend a transaction or business relations cannot be applied in relation to DNFBPs (c.40.12); • No requirement to obtain prior authorisation from the requested supervisor before disseminating information exchanged for prudential purposes (c.40.17); • LEAs' ability to exchange domestically available information and to apply available investigative techniques may be impacted by limitations under domestic law (c.40.18); • No explicit legal provisions regarding LEAs' powers to spontaneously share information on criminal property or to spontaneously identify and trace such

Recommendations	Rating	Factor(s) underlying the rating
		property (c.40.20); • LEAs' ability to conduct inquiries and obtain information on behalf of foreign counterparts may be impacted by limitations under domestic law (c.40.21); • No information regarding AML/CFT supervisors' ability to exchange information indirectly (c.40.24).

Glossary of Acronyms

	DEFINITION
AC Strategy	Anti-Corruption Strategy
ACC	Anti-Corruption Committee of Armenia
AMD	Armenian Money Dram
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism and Combatting the Financing of Proliferation of Weapons of Mass Destruction
AO Code	Code of Administrative Violations
AT	Assessment Team
BNI	Bearer-Negotiable Instrument
BO	Beneficial Ownership
BVI	British Virgin Islands
CARIN	Camden Asset Recovery Inter-Agency Network
CBA	Central Bank of the Republic of Armenia
CC	Criminal Code
CDA	Central Depository Agency
CDD	Customer Due Diligence
ChoA	Chamber of Advocates
CIS	Commonwealth of independent states
CMS	Case Management System
CPC	Criminal Procedure Code
CPREVC	Corruption Prevention Commission of Armenia
DLT	Distributed Ledger Technology
DNFBP	Designated Non-Financial Business or Profession
DPMS	Dealers in Precious Metals and Stones
DRA	Division for Religious Affairs
EAEU	Eurasian Economic Union
EDD	Enhanced Due Diligence
EMI	Electronic Money Institutions
EU	European Union
EUR	Euro
EWRA	Enterprise-Wide Risk Assessments
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FMC	Financial Monitoring Center of the Central Bank of Armenia
FSAP	Financial System Stability Assessment
FSLD	Financial Supervision and Licensing Department
FTZ	Free Trade Zone
GDP	Gross Domestic Product
GPO	General Prosecutor's Office of Armenia
IAC	Interagency Committee
IAIS	International Association of Insurance Supervisors
IC	Investigative Committee of Armenia
IMF	International Monetary Fund
IO	Immediate Outcome
IOSCO	International Organization of Securities Commissions
JD	Judicial Department of Armenia
JSC	Joint Stock Company
KRA	Key Recommended Actions
LACP Law	Law on Legal Assistance in Criminal Proceedings
LBS	Law on Banking Secrecy

LCFIA	Law on Civil Forfeiture of Illegal Assets
LEA	Law Enforcement Agency
LLC	Limited Liability Company
LOIA	Law on Operational Intelligence Activity
LP	Legal Person
LPSSO	Law on Payment and Settlement Systems and Payment and Settlement Organizations
MER	Mutual Evaluation Report
MIA	The Ministry of Internal Affairs of Armenia
ML	Money Laundering
MLA	Mutual Legal Assistance
MLAR	Mutual Legal Assistance Request
MLRO	Money Laundering Reporting Officer
MOE	Ministry of Economy of Armenia
MOF	The Ministry of Finance of Armenia
MOFA	Ministry of Foreign Affairs of Armenia
MOI	Ministry of Interior of Armenia
MOJ	The Ministry of Justice of Armenia
MOU	Memorandum of Understanding
MVTS	Money or Value Transfer Service(s)
NBFI	Non-Bank Financial Institutions
NCBC	Non-Conviction-Based Confiscation
NPO	Non-Profit Organisation
NRA	National Risk Assessment
NSS	National Security Service of Armenia
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Asset Control
OSINT	Open-Source Intelligence
PEP	Politically Exposed Person
PF	Proliferation Financing
PSO	Payment and Settlement Organisation
RBA	Risk-Based Approach
RE	Reporting Entity
RUR	Recommendation under review
SDD	Simplified Due Diligence
SRB	Self-Regulating Bodies
SRC	State Revenue Committee of the Republic of Armenia
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
TF	Terrorism Financing
TFS	Targeted Financial Sanctions
TTR	Threshold Transaction Reports
UBO	Ultimate Beneficial Owner
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNSCR	United Nations Security Council Resolution
UNTOC	United Nations Convention against Transnational Organized Crime
USD	United States dollar
VA	Virtual Asset
VASP	Virtual Asset Service Provider