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(2022)1

Anti-money laundering and counter-terrorist financing measures

Bulgaria

Fifth Round Mutual Evaluation Report

May 2022

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 fifth round mutual evaluation report on Bulgaria was adopted by the MONEYVAL Committee at its 63rd Plenary Session

(Strasbourg, 18 – 20 May 2022).

Contents

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and combating financing of terrorism (AML/CFT) measures in place in the Republic of Bulgaria (Bulgaria) as at the date of the onsite visit (6 - 17 September 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Bulgaria's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

a) Bulgaria has a reasonable understanding of the main money laundering (ML) risks and limited understanding of the terrorism financing (TF) risks, mainly based on the national risk assessment (NRA). The NRA contains a good initial analysis of the ML and TF threats Bulgaria faces; however, a lack of available and comprehensive statistical data, which varies from sector to sector, generally remains a significant impediment to risk assessment in Bulgaria. Bulgaria's ability to develop national AML/CFT policies to mitigate ML/TF risks is inhibited by the areas of risk understanding that require further improvement. Challenges exist in relation to inter-agency co-operation between LEAs, which is particularly hindered by the lack of necessary tools.

b) The lack of comprehensive statistics limits the authorities' understanding and their abilities to react to risks. Statistical data for evaluating the use of financial intelligence, investigation and prosecution of ML and TF and related predicate offences, confiscation and international cooperation are particularly limited.

c) Financial intelligence and related information is available to be accessed by the competent authorities, however, it is used in investigations and to develop evidence in relation to ML/TF and underlying predicate offences only to some extent. The timeliness and effectiveness of the use of financial intelligence and exchange of information is hampered by several technical and procedural limitations. In addition, the current system for reporting suspicious transactions does not ensure prompt reporting in all cases and creates potential tipping off issues. The general quality (and volume) of suspicious transactions reports (STRs) submitted by some sectors, especially by designated non-financial businesses and professions (DNFBPs) is insufficient.

d) The number of ML investigations, prosecutions and convictions and the severity of the criminal sanctions for ML is generally low compared to the number of registered predicate offences and is not commensurate with the identified ML risks of the country. Neither LEAs nor the prosecutorial authorities consider ML as a priority and there are no mechanisms in place to prioritize ML cases. The effectiveness of the system is hindered by the high threshold of evidence required for initiating formal pre-trial proceedings by the prosecution, complicated and redundant institutional framework, technical procedural constraints and lack of LEA staff with adequate expertise.

e) There is no legal or other mandatory requirement to pursue confiscation as a policy objective (e.g. by routinely launching parallel financial investigations or analyses). A number of technical issues hamper the confiscation and there is no mechanism available for the active management of seized assets beyond storage and safekeeping

measures. All authorities have difficulties with effectively securing, managing and recovering virtual assets (VAs) despite the frequent occurrence of such assets in case practice.

f) The authorities involved in the operative analysis, criminal investigation, and prosecution of terrorism-related and TF cases are adequately qualified, experienced, empowered and enabled to identify potential terrorism and TF risks. At the same time a generally low understanding of the TF risks by FIs and DNFBPs (with the exception of banks, payment institutions, e-money institutions and postal money operators) results in low-quality TF-related STRs, which in turn, generate low-quality FIU disseminations with little added value. The investigating and prosecuting authorities did not demonstrate that they take an effective and systematic approach to explore and investigate the financing aspects of the terrorism-related offences occurred. In addition, Bulgaria does not have a national countering terrorism (CT) or countering financing of terrorism (CFT) specific strategy and it was not demonstrated that TF investigations were integrated with, or supported by, other strategies involving CFT aspects or that outcomes of terrorism-related criminal proceedings would, in all cases, be sufficiently used for domestic and UN designations.

g) Bulgaria implements targeted financial sanctions (TFS) without delay through a combination of supranational and national mechanisms. No assets have been identified and frozen pursuant to the TFS to date. The NRA contains some analysis on the NPOs as a sector, identifying it as being vulnerable to TF abuse to some extent, however, the data collected for the purposes of TF risk assessment does not amount to comprehensive analysis on the activities and vulnerabilities of NPOs. The supervisory measures apply to all NPOs as opposed to NPOs with a higher risk.

h) Bulgaria implements proliferation financing (PF) related TFS through European Union (EU) regulations and thus is generally impacted by the delays between the designation decision taken by the United Nations Security Councils (UNSCs) and its transposition into the EU framework. All FIs and DNFBPs lack comprehensive understanding of their PF-related obligations. There is a robust export control regime targeting proliferation risks in Bulgaria with the central authority being the inter-ministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction. The activities *per se* also include PF issues, including checks with UNSCR related to PF.

i) Although supervisors are enhancing their risk-based supervisory models for financial sectors, DNFBP supervision is not risk based and is not effective. This can be attributed to a significant lack of resources in some supervisory authorities. The absence of market entry measures with a view to prevent criminals in real estate, accountancy, virtual asset service providers (VASPs) and trust and company service providers (TCSPs) sectors; as well as currency exchange offices (regarding beneficial owners (BOs), and the gambling sector (regarding higher BO threshold) is of concern, especially given the high level of organized crime (OC) and corruption in Bulgaria.

j) Knowledge of AML/CFT legal obligations by OEs is generally high and OEs conduct CDD on all clients, however, the majority of OEs need to advance their understanding of risks that are relevant to the nature of their business (beyond NRA) and enhance the application of preventative measures in higher risk areas and monitoring. Insufficient

risk understanding may limit OE's ability to identify suspicious activity and transactions which likely contributes to the low rates of suspicious activity reporting of both ML and TF.

k) Bulgaria has started implementing measures to increase transparency of the country's beneficial ownership regime. However, Bulgaria does not yet comprehensively understand the risks and vulnerabilities of different types of legal persons and arrangements. This has reduced the competent authorities' ability to implement more targeted mitigating measures to ensure transparency of the legal persons. Significant concerns are raised in relation to accuracy of the BO information held in the registers and availability of BO information held by the OEs.

l) Bulgaria provides generally timely and constructive assistance across the range of requests for international co-operation, including mutual legal assistance (MLA). The effectiveness of the international cooperation is affected by overly formal domestic cooperation procedures, extensive duplication of requesting international cooperation, deficiencies in the legislative framework regarding international legal cooperation with non-EU counterparts, deficiencies in relation to keeping BO information up to date and the absence of guidelines or clear procedures setting out the priorities for executing requests.

Risks and General Situation

2. Bulgaria' understanding of risks is mainly based on the national risk assessment of money laundering and terrorism financing risks (NRA). The main ML risk events identified by Bulgaria as a result of the NRA: laundering of funds from a range of foreign and domestic predicate offences linked to organised crime (primarily drugs, human trafficking and tax evasion) through the exploitation of the formal financial system and extensive use of cash; laundering the proceeds of corruption (particularly noting property and misuse of EU funds) through complex domestic and foreign-based ML layering schemes with assistance of ML professionals; laundering of funds from tax evasion and VAT fraud using straw men; integration of funds in the construction and real estate sector; laundering of funds from foreign predicate offences through non-bank investment intermediaries; laundering of illicit funds generated in the food and oil trade (tax fraud and evasion) using shell companies and informal nominees; laundering of funds from computer and social engineering fraud; and, involvement of ML professionals and reporting entities (due to vulnerabilities in market entry and employee screening).

3. The NRA analysis of the vulnerabilities is not yet sufficiently developed meaning that the analysis of residual risk is limited. The NRA also does not consider in sufficient detail the significant risks connected with a number of major predicate offences that require further detailed consideration – this includes but is not limited to: risk events linked to the laundering of proceeds of corruption; the use of domestic and foreign legal entities for obscuring beneficial ownership; the involvement of lawyers, accountants and notaries in facilitating ML; and, the potential abuse of investment-related residence and citizenship (IRRC) programme. The lack of detailed risk understanding in these areas inhibits the ability of Bulgaria to develop national AML/CFT policies to mitigate these risks.

4. According to the NRA, TF activity appears to be relatively restricted to the use of cash, money transfer services and the occasional use of illegal/informal financial services (*hawala*). Some TF risks have materialised in Bulgaria regarding the existence of limited financial and material support for foreign organisations functioning abroad and the use of *hawala* system as a conduit for support. The analysis of NPOs sector is limited and needs to be updated.

Overall Level of Compliance and Effectiveness

5. Bulgaria has made several amendments to its AML/CFT legislative framework after adoption of the previous Mutual Evaluation Report in 2019 to address the technical deficiencies identified. However, number of deficiencies remain. There are certain gaps related to domestic cooperation, preventative measures, supervisory mechanisms, dissuasiveness of the sanctions and TFS regime. These shortcomings present challenges for effectiveness.

6. Bulgaria achieves a moderate level of effectiveness regarding the assessment of ML/TF risks and domestic coordination, TF investigation and prosecution, TF preventive measures and TF related TFS, the implementation of preventive measures by FIs and DNFBPs, supervision of FIs and DNFBPs and international cooperation. Bulgaria demonstrates a low level of effectiveness in areas related to the use of financial intelligence, ML investigations and prosecutions, confiscation of criminals' proceeds of crime or property of equivalent value, PF related TFS and the prevention of misuse of legal persons and arrangements.

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

7. Bulgarian authorities have a reasonable level of understanding of the main ML risks Bulgaria faces based largely on the national risk assessment of the ML and TF risks completed in 2019 (NRA). The understanding significantly varies authority to authority and is hindered by limited vulnerabilities analysis, which is not yet sufficiently developed meaning that the analysis of residual risk is limited for certain sectors. Understanding is also hampered by obstacles, i.e. lack of detailed consideration of the significant risks connected with a number of major predicate offences (notably corruption, use of legal entities and professional enablers The NRA process covers generally the activities of VASPs and the potential misuse of legal persons for ML, however, Bulgaria is yet to comprehensively conduct a risk assessment of these areas.

8. TF risk in Bulgaria is understood to a limited extent by all authorities. It is currently limited to having a basic understanding of the cash economy in Bulgaria by the authorities and a developing understanding of how its geographical position may influence TF risk. Whilst figures exist on incoming and outgoing financial transfers there has been limited analysis of these figures, particularly considering high risk countries. Bulgaria has not conducted a proper and thorough TF risk assessment of its NPO sector.

9. Authorities understand potential for abuse of the IRRC programme by non-resident natural persons and how it can be abused for ML. The particular exposure of the IRRC to the laundering of corruption funds is acknowledged and understood. However, this understanding has not yet translated into appropriate policies to prevent against abuse of the IRRC.

10. Bulgaria faces major issues concerning co-operation and co-ordination at both a strategic level for developing and implementing policies for ML/TF and generally at an operational level. Risk understanding and co-ordination work is also hampered by the lack of suitable technology systems which can work on a multi-agency basis and lack of meaningful statistics in certain areas. The relatively recent development of risk understanding at a national level by authorities has only

very recently started to translate into national AML/CFT policies consistent with the risks identified, by virtue of actions that have started and are contained in the Action Plan. Several actions are already underway, with some having made significant progress. However, whilst some competent authorities have focussed on areas identified as higher risks in the NRA, generally the objectives and activities of the competent authorities are not yet consistent with the ML/TF risks identified. The lack of a National Strategy under which such policies can be developed is a significant shortcoming.

11. The assessment of risks is not properly used to justify all exemptions and support the application of enhanced and simplified measures. To the extent it is adequately used, this is only used to some extent.

12. The private sector has a general awareness of the NRA and its conclusions, however, engagement by the country with the private sector has been relatively minimal, therefore limiting their understanding of ML/TF risk. There has been limited outreach to NPOs, FIs and DNFBPs regarding NPO TF risks.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

13. Financial intelligence and related information are accessed, however, is used in investigations and to develop evidence in relation to ML/TF and underlying predicate offences only to some extent. The timeliness and effectiveness of the use of financial intelligence and exchange is limited by several technical and procedural limitations such as: the lack of suitable IT systems on inter-agency and multi-agency level; the major lack of human and technical resources allocated to the FID-SANS; no clear mechanism for dissemination of the FID-SANS information; limited feedback on use of financial intelligence by LEAs and prosecutors to the FID-SANS. The absence of clear procedures at OEs for the implementation of the postponement mechanism has an effect on the effectiveness of the work of the FID-SANS, as they result in all postponement STRs being handled with an utmost urgency.

14. The current system in place for reporting suspicious transactions does not ensure prompt reporting in all cases and creates potential tipping off issues. The general quality (and volume) of STRs submitted by some sectors, especially by DNFBPs needs improvement. The FID-SANS conducts strategic analysis to some extent, which only to a very limited extent support the needs of other institutions.

15. The number of ML investigations, prosecutions and convictions and the severity of the criminal sanctions for ML is generally low in Bulgaria compared to the number of registered predicate offences and not commensurate with the identified ML risks of the country. Neither LEAs nor the prosecutorial authorities consider ML as a priority and there are no mechanisms in place to prioritize ML cases.

16. The identification, investigation and prosecution of ML and major proceeds-generating offences is hampered by the complicated and redundant institutional framework, lack of LEA's staff with adequate expertise, lack of adequate technical resources and supervision over pre-investigative operation proceedings, absence of the procedures to examine routinely the financial aspects of the proceeds-generating criminality, high threshold of evidence required for initiating formal pre-trial proceedings by prosecution, including for ML cases related to foreign proceeds, and technical procedural constraints.

17. Lack of meaningful and detailed statistics diminish Bulgarian authorities understanding on the composition and characteristics of the ML criminality in the country and abilities to react to risks related to ML, associated predicate offences and TF.

18. Absence of statistics poses an insurmountable impediment to assessing the performance and effectiveness of the criminal (conviction-based) confiscation regime and the actual recovery of confiscated assets. There is no legal or other mandatory requirement to pursue confiscation as a policy objective (e.g., by routinely launching parallel financial investigations or analyses).

19. Number of technical issues hamper the confiscation, and in particular in major proceeds-generating offences, such as: short and strict statutory deadlines in pre-trial proceedings; absence of availability to confiscate from third parties in any other relations other than in ML and TF cases, including the provisional measures regime and the civil confiscation proceedings; the incompleteness of the cross-border cash control regime for stopping and restraining cash/bearer negotiable instruments (BNIs) transported through the internal borders of the EU. There is no mechanism available for the active management of seized assets beyond storage and safekeeping measures and for managing and disposing of property that has been confiscated under the Criminal Code (CC), bearing a direct impact on effectiveness particularly if more complex types of assets have to be managed. All authorities have difficulties to effectively secure, manage and recover virtual assets (VAs) despite the frequent occurrence of such assets in case practice.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

20. The authorities involved in the operative analysis, criminal investigation, and prosecution of terrorism-related and TF cases appear to be adequately qualified, experienced, empowered and enabled to identify potential terrorism and TF risks. However, generally low understanding of the TF risks by FIs and DNFBPs results in low-quality of TF-related STRs. This in turn generate low-quality FIU disseminations with little added value and the investigating and prosecuting authorities did not demonstrate to have an effective and systematic approach to explore and investigate the financing aspects of the terrorism-related offences occurred.

21. In addition, Bulgaria does not have a national CT or CFT specific strategy, instead of which CT (and to a lesser extent, CFT) elements are included in more general strategies. It was not demonstrated that TF investigations were integrated with or supported those strategies and that outcomes of terrorism-related criminal proceedings in all cases would be sufficiently used for domestic and UN designations.

22. Bulgaria implements the United Nations Security Council Resolutions (UNSCRs) 1267/1989, 1988 and 1373 without delay through a combination of supranational and national mechanisms. No assets have been identified and frozen pursuant to the sanctions regimes under UNSCR 1267/1989, 1988 or 1373, OEs demonstrated awareness of the TFS regime and confirmed that funds or other assets are identified, these would immediately be frozen. The proliferation financing (PF) related TFS is implemented through EU regulations and thus is generally impacted by the delays between the designation decision taken by the United Nations Security Council (UNSC) and its transposition into the EU framework.

23. All OEs showed at least a basic awareness of their obligations in relation to TF and PF-related TFS, but FIs, especially banks, demonstrated the most advanced understanding.

24. TF risks emanating from NPOs have not been comprehensively assessed in the NRA, targeting identification of the overarching risk environment in the sector and missing granularities – the features and types of NPOs which by virtue of their activities or characteristics,

are likely to be at risk of terrorist financing abuse. A registration framework for NPOs is in place, but no CFT focused, or risk-based measures have been developed and applied. Limited outreach conducted to the sector in relation to their TF risks.

Preventive measures (Chapter 5; IO.4; R.9–23)

25. All OEs demonstrate a generally high understanding of the AML/CFT obligations and are aware of the main national risks that are relevant to their businesses, namely - corruption risk and shadow economy linked to the prevalent use of cash. However, the level of understanding on how individual OEs can be abused for ML purposes varies (regarding FIs: banks, securities and investment had generally good understanding, payment institutions and e-money institutions lacked understanding of risks that were relevant to their nature of business and persons providing postal money orders (PMO), currency exchangers and other FIs had limited understanding). Regarding DNFBPs, real estate agents had generally good understanding, gambling operators and lawyers had reasonable understanding and understanding by TCSPs, and notaries was less well developed. VASPs demonstrated good understanding. Consequently, risk mitigation measures applied by OEs to address the risks also vary and is attributed to the varying levels of risk understanding. TF risk understanding is less developed for all sectors and is mainly limited to TFS screening obligations and high-risk country lists.

26. General customer due diligence (CDD) requirements are well understood by the OEs, including the requirement not proceed with business relationships and transactions in cases where satisfactory CDD was not obtained. However, some OEs face difficulties in verifying beneficial owners of the customers, especially those that form complex ownership structures. Some non-banking FIs and DNFBPs rely on CDD conducted by banks to a certain extent by assuming transactions conducted through banks can be trusted as they are subject to close scrutiny.

27. Although enhanced customer due diligence (EDD) requirements are well understood by the OEs, the level of application and scrutiny thereof vary. EDD is commonly applied to high-risk countries and PEPs, however, limited consideration is given to other high-risk circumstances. The low number of high-risk clients relative to the size and scale of the business is a concern, especially in the banking sector given its materiality and risk exposure.

28. All OEs have measures in place to identify PEPs, however, verification mechanisms vary. Difficulties were noted regarding verification of source of funds (SOF) and source of wealth (SOW) information, as well as development of distinct monitoring scenarios to monitor PEP client in an enhanced manner. Varying degrees of understanding have been demonstrated by the OEs to implement TFS related to TF, with banks demonstrating the highest level of knowledge. Although all OEs apply specific and enhanced measures towards high risk third countries, it is not evident that clients from high-risk jurisdictions and transactions are monitored in an enhanced manner. A lack of understanding of what to look out for in order to identify suspicion by the OEs leads to deficiencies in monitoring that translate into the low reporting rates by the OEs, except banks and other payment service providers. This highlights the need for sector specific guidance to identify suspicion, especially in the TF field.

29. Internal control and compliance arrangements in the OEs appear to be proportionate to the OE's size. None of the OEs reported that technical compliance gaps (see TCA) have any impact on their ability to comply in practice.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

30. The Financial Supervision Commission (FSC) and the Bulgarian National Bank (BNB) apply controls to prevent criminals from owning or controlling the entities they supervise; however, no fit and proper tests are performed on shareholders of currency exchange offices and entry controls for shareholders in the gambling sector are applied at a higher threshold than is permitted by the FATF standard. PMO operators are subjected to limited market entry requirements and real estate agents, virtual asset service providers (VASPs), trust and company service providers (TCSPs) and accountants are not subject to any. Processes of ongoing monitoring for compliance with the entry requirements and detection of close associates of criminals require substantial enhancement.

31. Financial supervisors demonstrate fair knowledge of ML risks in their supervised sectors. The primary AML/CFT supervisor, the FID-SANS, demonstrates understanding of general ML risks which is mainly focused on the ML risk events the country is facing as identified in the NRA, rather than risks and vulnerabilities that individual sectors are facing. TF risk and institutional risk understanding is less developed across all supervisory authorities. The National Revenue Authority (NaRA) seems to underestimate the risks in its supervised gambling and currency exchange sectors; the CRC being a supervisory authority of PMOs is unable to clearly articulate vulnerabilities and risk exposure of the postal money remittance sector.

32. Whilst financial supervisors are taking positive steps with developing risk-based supervisory models, further enhancement is required, especially in relation to institutional risk assessment, i.e., scope and depth of analysis required to conclude on the risks that individual supervised financial institutions are facing. That is especially a concern in banking and MVTS sectors due to their materiality and risk exposure.

33. DNFBP supervision is not risk-based and a very low number of inspections of DNFBPs have been carried out by the FID-SANS to check the compliance with AML/CFT requirements. Inspections of postal money order providers conducted by the CRC have limited effectiveness as they extend only to offsite reviews of internal procedures which is concerning given the materiality and risk exposure of this sector. Regulation and on-site supervision of VASPs are in the infancy stage. Supervision of gambling is under development by the NaRA following the cessation of the former regulator, the SGC.

34. In general, shortage of resources (human, technical and financial) in supervisory authorities (except the BNB and the FSC), especially the FID-SANS, limits the efficiency of the risk-based supervision in terms of the frequency and scope/depth of checks for both, on-site inspections, and off-site reviews; as well as guidance and outreach measures.

35. The AML/CFT sanctioning regime is not proportionate, dissuasive, and effective. There is a prevalence of cases whereby fines are imposed but not settled. Objectiveness of judgement by the supervisory authorities on the level of severity and systemic nature of the breaches is at times questionable. Supervisory authorities have not issued sanctions for infringements in the TFS related to TF area, as supervisors claim never to have identified severe breaches.

36. Supervisory authorities could not fully demonstrate that they make an impact on obliged entities level of compliance with AML/CFT. Instances of repeat infractions by the individual obliged entities, as well as common violations per sector are noted throughout the whole review period (2015-mid-2021).

37. There is lack of sector specific guidance to promote understanding by the obliged entities of AML/CFT and TFS obligations, especially concerning monitoring and identification of

suspicious activities and transactions. Supervisory guidance is essential for the most material sectors (banks and MVTS), as well as new or rapidly developing sectors such as online gambling and VASP. No aggregated supervisory feedback is provided on common infractions identified through inspections and/or very little on sectorial and institutional risks.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

38. Bulgaria has conducted a high-level analysis of the risks associated with the legal persons as part of the NRA exercise in 2020. The risk assessment acknowledges use of the LLC structures as particularly vulnerable to abuse, including prevalent use of strawmen and shell companies in ML schemes. However, given the general nature of the analysis, the precise nature and extent of the risks and particularly the vulnerabilities of all types of legal person are not yet understood. This hampers the level of understanding by the competent authorities of the systemic vulnerabilities and the extent to which legal persons created in Bulgaria can be or are being misused for ML/TF; consequently, it negatively affects the country's ability to effectively mitigate risks related to legal persons and arrangements.

39. Significant issues exist with an exercise Bulgaria has undertaken to convert bearer shares into registered shares by mid-2019, the exercise has not been completed to date and 40% of companies are still to convert shares. Very limited action has been taken by Bulgarian authorities against those who have failed to convert shares. Whilst Bulgaria does not provide for the existence of formal nominees in legislation, there are no verification mechanisms to check for nominee arrangements. However, even in a situation where nominee arrangements were found, there is no legal prohibition for their existence and thus no legal grounds to initiate proceedings.

40. The Bulgarian authorities use a combined approach to ensure basic and BO transparency of the legal persons created in Bulgaria, namely: through information on the various registries which hold beneficial ownership information; through the obliged entities – mostly banks; through the legal entity itself and/or the natural person contact point. However, all of these methods have serious shortcomings that hinder reliability and accuracy of BO information.

41. It can't be ascertained, that beneficial ownership data can be obtained from the OEs in all cases: although the legal persons are legally required to deposit share capital into the Bulgarian bank by opening the account before registering legal person, this requirement does not extend throughout the lifetime of the legal person; legal persons are not legally required to engage a TCSP (lawyer and/or accountant) to register a company; moreover, the statistics on how many Bulgarian registered legal persons have sought services of the TCSPs in Bulgaria are not known. Even in cases where beneficial ownership information is available from the OEs, the evidence, based on the shortcomings that relate to the implementation of the BO legal requirements by the OEs, suggests that BO data held by OEs might not be always reliable. Moreover, the supervisory regime is not fully effective which further hamper reliability of BO information held by the OEs. Linked to this, a regulatory regime for TCSPs is not established in Bulgaria and the exact population of lawyers and accountants conducting TCSP and other activities covered by the FATF standard is not known.

42. In 2018, Bulgaria introduced provisions in the legal acts which provide the legal basis for setting up of a BO registry. However, no verification checks are conducted on the accuracy and how up to date the beneficial ownership information is which is held on the registries. The effectiveness of the Registry Agency in administering the relevant registers is significantly hampered by the lack of resources: human, technical, and financial. Significant issues exist in relation to discrepancy reporting with a very low number of discrepancy reports filed and there

are significant issues in taking action to amend the Register. The AT were not able to ascertain if the Register has ever been amended (despite discrepancies) and which agency can amend the Register.

43. Sanctions applied against persons who do not comply with the basic and beneficial ownership information requirements are not effective, proportionate, and dissuasive and very few sanctions were applied in the relevant period.

International cooperation (Chapter 8; IO.2; R.36–40)

44. Bulgarian legislation sets out a comprehensive legal framework for international cooperation in criminal matters, which enables the authorities to provide a broad range of assistance concerning ML/TF and associated predicate offences. The MoJ serves as the central authority for international cooperation in MLA requests in the trial stage in Bulgaria. In the pre-trial stage foreign MLAs (including European Investigative Orders (EIOs)) are executed by prosecutors, where central authority is the General Prosecutors Office. In cases of criminal proceedings channels of cooperation through direct communication are used by the MoI (Police) and the FID-SANS with respective foreign partners.

45. Bulgaria provides generally timely and constructive assistance across the range of requests for international co-operation, including mutual legal assistance (MLA). The effectiveness of the international cooperation is affected by certain technical and procedural deficiencies, which in practice, however, have not yet created major obstacles to provide timely and constructive international legal assistance to foreign counterparts.

Priority Actions

Bulgaria should address following priority actions:

a) Increase the understanding of authorities on national level of ML/TF risks and translate that understanding into national AML/CFT policies under the umbrella of a national AML/CFT strategy. Develop better systems to collect sufficient statistics that would support NRA conclusions and further risk understanding work and urgently reconsider the status, structure, and resources of the NRAM WG to ensure its ability to co-ordinate the development and implementation of policies and activities to combat ML/TF and PF effectively.

b) Take measures to enhance the FID-SANS analysis (both operational and strategic) and dissemination functions, as well as the subsequent financial intelligence functions of LEAs, including increasing the human, IT and other necessary resources of authorities performing financial intelligence activities.

c) Reconsider the institutional framework for identifying and investigating ML particularly in terms of redundant competencies and ensure that ML should be considered a priority by LEAs and prosecutorial bodies with having necessary strategy or policy to apply risk-based approach. Increase the technical resources and specialization within LEAs and revisit the formalistic and bureaucratic characteristics of the Criminal Procedures Code (CPC) starting with the deadlines in Art. 234 of the CPC and revising the sanctions regime.

d) Urgently remedy the technical deficiencies relating to seizure and confiscation regime and introduce clear requirements to pursue parallel financial investigations with clear and updated methodological guidance for the practitioners.

e) Issue a national strategy specifically on CT and CFT related issues. Enhance the FID-SANS' in-depth analysis of TF-related STRs and provide the FID-SANS with sufficient resources and expertise. Ensure that detection and investigation of all financing aspects are carried out in a systematic manner for all terrorism-related offences, extending to all forms of TF.

f) Urgently develop adequate mechanisms and procedures for delisting and unfreezing with regard to UNSCRs 1276 and 1988. Conduct an in-depth risk assessment of the NPO sector to form an objective analysis of risks posed by the sector based on underlying comprehensive assessment of all characteristics and statistics to identify those NPOs at risk from terrorist abuse and apply targeted supervision or monitoring towards those at risk, without hampering legitimate NPO activity.

g) Expand the scope of national mechanism to combat proliferation or introduce a separate PF dedicated mechanism for the coordination and implementation PF related TFS without delay. Ensure adequate supervision and monitor PF-related TFS.

h) Establish market entry measures with a view to prevent criminals and their associates for currency exchange (regarding BOs), real estate, accountancy, VASPs and TCSPs sectors and gambling sector (regarding higher BO threshold) and take proactive measures to prevent unlicensed *hawala* businesses.

i) Implement urgent measures to strengthen supervision with AML/CFT requirements by the DNFBPs and strengthen supervision of ML/TF monitoring, STR reporting requirements and TFS across all sectors.

j) Define and develop a clear nation-wide strategy and guidelines (including set priorities) to ensure systematic proactive and adequate seeking of foreign assistance in line with the investigative priorities. Establish a clear procedure to streamline cases with a foreign nexus, to avoid repetitively seeking assistance in stages of analysis, pre-investigation, and investigation.

k) Urgently review policies concerning the accuracy of beneficial ownership information on the registers, the role of the Registry Agency and establish more robust mechanisms concerning accuracy of information on the central register along with a more detailed understanding of how LPs and LAs are being or may be misused for ML/TF. Urgently take action to achieve the full registration of the remaining 40% of Joint Stock Companies (JSC) bearer shares.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[1]

IO.1 – Risk, policy and coordination	IO.2 – International cooperation	IO.3 – Supervision	IO.4 – Preventive measures	IO.5 – Legal persons and arrangements	IO.6 – Financial intelligence
ME	ME	ME	ME	LE	LE
IO.7 – ML investigation & prosecution	**IO.8 – Confiscation**	**IO.9 – TF investigation & prosecution**	**IO.10 – TF preventive measures & financial sanctions**	**IO.11 – PF financial sanctions**	
LE	LE	ME	ME	LE	

Technical Compliance Ratings[2]

R.1 – assessing risk & applying risk-based approach	R.2 – national cooperation and coordination	R.3 – money laundering offence	R.4 – confiscation & provisional measures	R.5 – terrorist financing offence	R.6 – targeted financial sanctions – terrorism & terrorist financing
LC	PC	LC	PC	PC	PC
R.7- targeted financial sanctions - proliferation	**R.8 -non-profit organisations**	**R.9 – financial institution secrecy laws**	**R.10 – Customer due diligence**	**R.11 – Record keeping**	**R.12 – Politically exposed persons**
PC	PC	LC	PC	LC	PC
R.13 – Correspondent banking	**R.14 – Money or value transfer services**	**R.15 – New technologies**	**R.16 – Wire transfers**	**R.17 – Reliance on third parties**	**R.18 – Internal controls and foreign branches and subsidiaries**
PC	PC	PC	LC	C	PC
R.19 – Higher-risk countries	**R.20 – Reporting of suspicious transactions**	**R.21 – Tipping-off and confidentiality**	**R.22 - DNFBPs: Customer due diligence**	**R.23 – DNFBPs: Other measures**	**R.24 – Transparency & BO of legal persons**
LC	LC	LC	PC	LC	PC
R.25 - Transparency & BO of legal arrangements	**R.26 – Regulation and supervision of financial institutions**	**R.27 – Powers of supervision**	**R.28 – Regulation and supervision of DNFBPs**	**R.29 – Financial intelligence units**	**R.30 – Responsibilities of law enforcement and investigative authorities**
PC	PC	PC	PC	LC	LC
R.31 – Powers of law enforcement and investigative authorities	**R.32 – Cash couriers**	**R.33 - Statistics**	**R.34 – Guidance and feedback**	**R.35 - Sanctions**	**R.36 – International instruments**
C	PC	PC	PC	PC	LC
R.37 – Mutual legal assistance	**R.38 – Mutual legal assistance: freezing and confiscation**	**R.39 – Extradition**	**R.40 – Other forms of international cooperation**		
LC	PC	LC	LC		

[1] Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

[2] Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant.

MUTUAL EVALUATION REPORT

Preface

1. This report summarises the AML/CFT 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 system and recommends how the system could be strengthened.

2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 6-17 September 2021.

3. The evaluation was conducted by an assessment team consisting of: Mr George Pearmain, Director of Financial Crime Strategy, Department for the Economy, Government of Jersey (*financial expert*); Ms Helen Ault, Director of Isle of Man Gambling Supervision Commission (*financial expert*); Mr Toms Platacis, Deputy Head of the Financial Intelligence Unit of Latvia (*law enforcement expert*), Mr Lajos Korona, Public Prosecutor, Head of Division, Metropolitan Prosecutor's Office of Hungary (*legal expert*); Ms Zaruhi Badalyan, Methodologist and Legal advisor, Legal Compliance Division, Financial Monitoring Centre, Central Bank of Armenia (*legal expert*); with the support of MONEYVAL Secretariat: Ms Veronika Mets, Administrator, Ms Kotryna Filipaviciute, Administrator and Ms Laura Kravale, Administrator. The report was reviewed by FATF Secretariat, Mr Fabian Rieger, Policy Advisor Anti-Money Laundering & Counter-Terrorism Financing, Federal Ministry of Finance, Germany and Ms Mira Katz Atias, Operational and Policy Analyst, Israel Money Laundering and Terror Financing Prohibition Authority.

4. Bulgaria previously underwent a MONEYVAL Mutual Evaluation in 2013, conducted according to the 2004 FATF Methodology. First follow-up report was adopted in September 2015, second in September 2016, third in June 2017, fourth in December 2017 and first compliance report in July 2018. The 2013 evaluation report and 2018 first compliance report has been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/bulgaria.

5. That Mutual Evaluation concluded that the country was compliant (C) with 11 Recommendations; largely compliant (LC) with 27 Recommendations; partially compliant (PC) with 9 Recommendations; not applicable (N/A) with 1 Recommendation and had no non-compliant Recommendations. Bulgaria was rated C or LC with 11 of the 16 Core and Key Recommendations.

6. Following the adoption of the 4th round MER in September 2013, Bulgaria was placed in regular follow-up. Bulgaria's fourth follow-up report in December 2017 concluded that, despite positive steps undertaken, some deficiencies with regard to one core recommendation (SR.II) and one key recommendation (R.3) were still in place. Consequently, the 55th Plenary placed Bulgaria under the Compliance Enhanced Procedures (CEPs) Step 1. The 56th Plenary concluded that Bulgaria brought all outstanding core and key recommendations to a level of LC, as required by the removal-conditions in Rule 13, paragraph 4 of MONEYVAL's 4th round rules of procedure and removed Bulgaria from the CEPs in July 2018.

1. ML/TF RISKS AND CONTEXT

7. Bulgaria is situated in southeast Europe and is bordered by Romania to the north, Serbia and North Macedonia to the west, Greece and Turkey to the south, and the Black Sea to the east. The territory of the country is 110 879 square km. The capital of Bulgaria is Sofia. As of 2020 the population of the country is approximately 6.92 million.

8. The Republic of Bulgaria is a parliamentary republic and pursuant to its constitution the State power is shared among the legislative (National Assembly), the executive (Council of Ministers and the bodies of local self-government) and the judicial (courts, prosecutor's offices, and investigative authorities) branches of the government. The President is the head of State that embodies the unity of the nation and represents the Republic of Bulgaria in international relations. The country is a unitary state, divided into 28 provinces. The legal system in Bulgaria is based on the civil law system.

9. Bulgaria is the sixteenth-largest country in Europe and is a Member State (MS) of the European Union (EU) since 1 January 2007. The country is not part of the Schengen Area and has checkpoints across all its borders. Bulgaria has an upper-middle-income economy[3] and its market economy is part of the European Single Market and is largely based on services, followed by industry and agriculture.

1.1. ML/TF Risks and Scoping of Higher Risk Issues

1.1.1. Overview of ML/TF Risks

ML risks

10. According to the National Risk Assessment (NRA), conducted by Bulgaria in 2019, organised crime offences trafficking in human beings or narcotics, and the trade of counterfeited goods, such as cigarettes, alcohol, and fuel, as well as tax crimes and fraud (including online and VAT fraud) appear to be the predominant predicate offences for ML schemes in Bulgaria.

11. *Corruption*: The NRA report has placed corruption-related ML risks among the top-tier of risk scenarios based on the significant estimated size of the corruption phenomenon and the consequences that it has on the state, economy and society.

12. *Organized Crime:* A large proportion of proceeds-generating offences falling under the predicate category in Bulgaria are within the scope of organised criminal activities in their various forms.

13. *ML of foreign predicates:* The geographic factor with regard to cross-border cash movement poses one of the key risks. Bulgaria has an external East and South border of EU and the risk of ML and TF through money flows from the neighbouring countries affected by complex geopolitical conflicts as the countries from the Middle East, North Africa, Eastern Europe (especially countries at the EU borders), remains high. The 2019 NRA identified cross-border movement of funds (TF risk) and cross-border movement of cash and precious metals and stones (ML risk) as significant ML/TF risks.

[3] Data for Upper middle income, Bulgaria | Data (worldbank.org)

14. *Professional ML* is conducted by professional money launderers both within organised crime groups and those acting autonomously. The latter set up complex legal structures and operate accounts both domestically and abroad. Natural persons tend to act "s*traw men*"/nominees for criminal enterprises and PEPs. In terms of quantity the majority of natural persons in ML cases are associated with online fraudulent activity usually linked to internet scams which tend to be high in volume but low in value, thus posing a medium risk. In these scenarios resident natural persons are generally used as "*straw-men*" to receive/collect the proceeds generated by online fraud and other offences and transfer those abroad via large international MVTS providers. A large number of ML cases with natural persons involve tax crimes as the predicate offence (VAT fraud), with the highest risk business sectors being the food trade, followed by the trade in petroland petroleum products (fuels) and the scrap metal trade. Natural persons are extensively involved in the smuggling of cash across the border from a variety of predicate offences. There is a risk that representatives of the legal and accounting professions could be associated with this type of activity.

15. *Non-resident natural persons*: The risk events identified by Bulgarian authorities in this context tend to be predominantly associated with transnational (computer) fraud cases. Additional ML risk for non-resident natural persons relate to the investment-related residence and citizenship (IRRC) programme. Furthermore, non-resident natural persons are extensively engaged in the physical cross-border transportation of cash along the Balkan route and represent both ML and TF risks.

16. *Non-resident PEPs:* A key risk scenario with regard to non-resident PEPs and non-resident natural persons is the use of associates for laundering corruption-related funds through investment in liquid assets or occasionally, participation in privatisation, as well as the investment-related residence and citizenship (IRRC) programme. The latter allows non-residents to obtain a fast-track to residency and citizenship based on investment in Bulgaria, including government bonds. The IIP carries specific risks of integration of funds of criminal origin in Bulgaria, as well as layering of funds through Bulgaria (e.g. after a 5 year period the bonds investments are paid out).

17. *Domestic PEPs:* Although the data is inconclusive there are a number of indicators that domestic PEPs represent a high risk for ML, which includes placement and layering of funds abroad including in offshore zones and their subsequent integration in the EU and Bulgaria through a number of schemes. This is one of the highest risk factors identified by the NRA, given that the consequences have the potential to lead to political and social destabilisation.

18. *Trade based money laundering (TBML):* The economic sectors most susceptible to ML activity tend to be those involved with fuels and mining, wholesale and retail trade, real estate, transport, and agriculture in the context of fraud with EU funds. Small and mid-sized companies tend to be more susceptible to ML risks as they are not as strictly monitored by oversight bodies in the same way that larger enterprises are. An illustrative example of this can be found in the real estate sector which is not subject to licensing and registration requirements and does not have an effective self-regulating mechanism. As such, it exhibits a higher degree of vulnerability as a conduit of illicit funds. Economic sectors tend to be abused for different purposes in the ML cycle, with the trade sector primarily utilised in the TBML context for ML layering, while real estate is primarily used for ML integration.

19. *Embezzlement of public funds/EU funds:* A significant proportion of the Bulgarian economy is dependent of state and budgetary expenditures and various types of public

procurement and public works, which are associated with potential for embezzlement by PEPs and potentially involved parties in the private sector. Another significant source of funding associated with various fraud are the EU funds. In this sense the public sector is potentially a major generator of criminal proceeds, which are subsequently placed and layered through a range of avenues. The construction sector receiving the largest public expenditure faces the dual threat of procurement fraud/embezzlement and ML integration schemes.

TF risk

20. According to the NRA, TF activity appears to be relatively restricted to the use of cash, money transfer services and the occasional use of illegal/informal financial services (*hawala*). Some TF risks have materialised in Bulgaria regarding the existence of limited financial and material support for foreign organisations functioning abroad and the use of *hawala* system as a conduit for support. The analysis of NPOs sector has been conducted but it needs to be updated.

1.1.2. Country's Risk Assessment & Scoping of Higher Risk Issues

21. Bulgaria completed its first holistic NRA of ML and TF risks in 2019 using methodology designed by the Council of Europe (CoE). The NRA includes following components: (i) analysis of threats; (ii) analysis of subjects undertaking ML; (iii) analysis of economic sectors associated with ML; (iv) analysis of financial/DNFBP sectors and products abused for ML and TF; (v) analysis of cross-border characteristics of ML; and (vi) analysis of TF risks.

22. The NRA was led by the standing interdepartmental working group (permanent interagency working group) (NRAM WG) established by the Council of Ministers (CoM). This group is a successor of the *ad-hoc* interdepartmental working group established by joint Ordinance Co-Chaired by the SANS (through the Head of the FID-SANS) and the Ministry of the Interior (through the Head of the AML Unit of the General Directorate of the Combatting Organised Crime). All relevant stakeholders from government, law enforcement, intelligence agencies, supervisors, and the private sector participated in the NRA assessment (with the exception of the Communications Regulation Commission). Sources used include public national and international reports in the relevant areas, including from Europol, the FATF, MONEYVAL and the EU Supranational Risk Assessment of ML and TF (SNRA). See IO.1 on further details, including deficiencies regarding the country's risk assessment.

Scoping of Higher Risk Issues

23. The AT identified following areas which required an increased focus through an analysis of information provided by the Bulgaria on its national ML/TF risks (as outlined above), and information from reliable third-party sources (e.g. reports by governments or other international organisations). The assessors focused on the following issues which were to some extent consistent with the findings of the NRA:

- ***Organized Crime*:** Organised criminal groups (OCGs) are engaged in a range of criminal activities in Bulgaria, focused mainly on trafficking of drugs, human trafficking and sexual exploitation, crimes against property, organised VAT and EU funds fraud and cybercrime. The AT assessed whether authorities are effectively fighting organised crime.

- ***Corruption*:** NRA acknowledges corruption as one of the main ML predicate offences in Bulgaria. The AT focus was put on the measures applied by obliged entities (OEs) regarding their clients who are politically exposed persons (PEPs). AT also evaluated whether the measures in place to fight corruption and related ML are effective and discussed the possible challenges that

law enforcement agencies (LEAs) and prosecutors may face in relation to investigating and prosecuting cases related to PEPs/high level officials. The evaluators gave particular focus to outcomes of suspicious activity reports (STRs) relating to PEPs that have been disseminated to law enforcement.

- ***Other ML events/predicate offences**:* NRA has identified in addition to corruption and OCGs issues also following ML events of higher concern: (i) integration of significant amounts of laundered funds in the construction sector and investment in real estate in the context of a significant share of informal economy by domestic and foreign perpetrators; (ii) laundering of funds from foreign predicate offences through non-bank investment intermediaries in Bulgaria is complemented by cases of unregulated activities involving securities; (iii) laundering of illicit funds generated in the food and oil trade (tax fraud and evasion) using shell companies and informal nominees (straw men) and relying on a corrupt environment and informal economy; (iv) laundering of funds from computer and social engineering fraud perpetrated by small-to-medium organised criminal groups using Bulgarian territory for layering of the funds; (v) Possible involvement of professionals and reporting entities (facilitated by market entry and employee screening vulnerabilities) is observed as a major risk that enables organised crime to function and thus contributes to most of the aforementioned risks. AT analysed whether ML investigations, prosecutions, convictions and confiscations are in line with these most significant predicate offences to ML and sector specific vulnerabilities.

- ***Terrorist and Proliferation Financing*:** NRA has identified following higher areas of concern in relation to TF: (i) use of MVTS and informal value transfer system (hawala) to transfer funds potentially related to TF and facilitation by migrant communities aggravated by large cash-based and informal economy; (ii) potential risk (to a limited extent) of diverting funds allocated for non-profit organizations (NPO) or religious activities in Bulgaria towards TF. The AT examined the mechanisms to combat TF, including whether TF cases have been properly investigated and where necessary prosecuted and weather OEs apply appropriate measures to prevent TF. For proliferation of financing (PF) the focus is on the application of relevant UNSCRs. The AT focussed on the use of indirect channels for money transfer for TF purposes and measures applied to NPOs which are vulnerable to TF risk.

- ***Shadow economy and the use of cash***: NRA acknowledges the risk of ML emanating from the widespread use of cash in several sectors, related to informal economy and cross border movements. AT examined the measures to mitigate the risks emanating from the widespread use of cash.

- ***Preventative measures**:* The AT assessed the understanding of domestic and cross-border ML and TF risks by OEs, their understanding and implementation of reporting obligations and managing of ML/TF risks, giving special attention to high-risk and more material sectors, such as banks, MVTS, real estate, etc. The AT examined the grounds why ML risks for currency exchange, and post operators were in NRA evaluated to be lower and consideration given to newly emerging sector risks, particularly virtual assets services providers (VASPs).

- ***Supervision*:** The AT focused on assessing the priorities, available resources, application of risk-based approach and implementation of sanctions by supervisory authorities. The AT also examined how well are the supervisory activities managed and coordinated, particularly regarding joint inspections and the new gambling supervisor, whether supervisory measures and sanctions have been effective.

- ***Resource Sufficiency of the Competent authorities***: The NRA identifies that the resource sufficiency of the competent authorities has had a significant impact on the efficiency of the competent authorities in fulfilling their functions. This is particularly noted to be the case in the area of corruption noted as the most extreme risk in the NRA. The AT therefore examined the sufficiency of resource across the competent authorities but particularly in FID-SANS, the law enforcement and judicial authorities with regard to identifying, investigating and prosecuting corruption, carrying out asset recovery, and investigating complex ML cases.

- ***Misuse of Legal Persons*:** Legal persons resident in Bulgaria represent the second highest number of subjects involved in potential ML activity, with the average volume of cases significantly higher than for natural persons. This particularly involves legal persons involved in cash-based operations, particularly concerning Limited Liability Company (LLCs) with a single "straw man" as owner. These structures involve the mingling of licit and illicit funds and enable access to the Bulgarian financial system and tend to be used as parties to fictitious loan agreements involving offshore companies or in trade-based ML schemes. LLCs are also often used as "shelf" or "shell" companies and are offered to and misused by EU-resident persons for tax evasion/tax fraud or related ML purposes. In this context legal persons pose a significant vulnerability to abuse by PEPs and PEP-related criminal groups for complex money laundering schemes through third countries. Bulgaria also has exposure to complex ML schemes often involving legal persons incorporated in Bulgaria whose ownership and management is linked to offshore companies or shell companies located in other EU MS. The AT focused on the extent to which legal persons are misused for ML/TF and particularly focused on how they can be used to layer licit and illicit funds and provide access to the Bulgarian financial system. The AT considered how LLCs can be used as "*straw man* entities" and also as "*shelf*" or "*shell*" companies. The AT also examined how LLCs may misused by EU-resident persons for tax evasion/tax fraud or related ML purposes. Finally, the AT considered the misuse of foreign legal persons active in Bulgaria, particularly from countries and jurisdictions with no requirements for maintaining such information in centralised registers with public access.

1.2. Materiality

24. The national currency of the Republic of Bulgaria is the Bulgarian Leva (BGN) which has a fixed exchange rate against the Euro of €1 to BGN 1,95583. In 2020 the nominal gross domestic product (GDP) in Bulgaria was 119 951 million BGN (61 330 million EUR) and the GDP per capita was 17 290 BGN (8 840 EUR).

25. In 2019, the real GDP per capita was € 6 630 and the GDP at 2015 prices was € 51.8 billion. In 2020, the real GDP per capita was € 6 380 and the GDP at 2015 prices was € 49.5 billion. According to data provided by the National Statistics Institute, Bulgaria's GDP grew by 4% in 2019 and declined by 4.4% in 2020. The main sector of the economy is services (61.3% of GDP in 2020) and particularly wholesale and retail trade, transportation, accommodation and food services (18.6% of GDP in 2020). Mining, manufacturing, electricity, gas and water supply accounted for 17.7% of GDP in 2020 and construction was 4.3% of GDP. The share of sector of public administration and defence; compulsory social security; education; human health and social work activities increased from 12.5% of GDP in 2019 to 14.5% in 2020, while financial and insurance activities dropped to 4.9% of GDP in 2020, being 5% in 2019.

26. Bulgaria has the highest proportion of the shadow economy to GDP among EU jurisdictions, standing at 29.6% based on most recent IMF research.[4] This is a major factor in large-scale tax evasion, particularly of value-added tax (VAT) and excise duties. Evasion of social security payments, through unreported income and informal employment arrangements, continues to be widespread. A large proportion of the sectors of construction, housing and informal enterprises are informally organised, because of light regulation in these sectors.

1.3. Structural elements

27. Bulgaria has some of the main structural elements in place for an effective AML/CFT system, including political and institutional stability, government accountability, separation of state powers and a capable and independent judiciary.

1.4. Background and Other Contextual Factors

28. Bulgaria ranks 53 for Rule of Law Index in 2020[5] and 69 in the Corruption Perceptions Index 2020[6] and experiences the worst levels of corruption in the European Union, a phenomenon that remains a source of profound public discontent. In the Bulgarian context corruption is both a contextual factor and potentially one of the significant proceeds generating offence. In addition, the risk of organised crime remains high in Bulgaria together with the risk related to "*professional money launderers*". Bulgaria has also investment-related residence and citizenship (IRRC) programme, that enables foreigners to acquire EU citizenship by obtaining a Bulgarian passport.

29. The territory of the Republic of Bulgaria is part of an established trade and transportation corridor between the Middle East and Europe known as the '*Balkan Route*'. The route is used for criminal purposes, such as the smuggling of goods and the trafficking of drugs, people, arms, and both licit and illicit goods and assets transit this route usually towards and from Central/Western Europe or North-Eastern Europe and the Middle East and Asia. The consequences of its geographical position mean that Bulgaria experiences a variety of predicate offences transiting its territory, the perpetrators of which abuse a number of financial and non-financial sectors. The Balkan route is also a corridor for the transportation of large volumes of cash across the borders to and from Europe, accompanied by the occasional use of *hawala* systems for TF purposes related to the recent migration flows.

30. Cash remains an issue of concern as it is used across sectors and businesses to perpetrate a variety of predicate offences. It also appears to be the predominant type of asset laundered. In this context the vulnerabilities in application of AML/CFT preventative measures by some obliged entities and the large informal economy allow cash of illicit origin to enter the formal financial system.

31. Bulgaria is subjected to global and regional risks in the context of the current global threat of terrorism. The position of the country also provides for its transit role on the route of foreign terrorist fighters, legal and illegal migration related to conflict zones, the regional situation, including unresolved disputes in neighborhood countries.

---

[4] Shadow Economies Around the World: What Did We Learn Over the Last 20 Years? (imf.org). The paper covers the period 1991–2015 and the proportion of the shadow economy is an estimation.
[5] WJP Rule of Law Index 2020 | World Justice Project
[6] 2020 Corruptions Perceptions Index - Explore the… - Transparency.org

1.4.1. AML/CFT strategy

32. In 2019 Bulgaria has taken legislative actions to prevent the possibility of using the financial system for the purpose of ML and TF (see para 35). Furthermore, actions have been also taken to mitigate the risks of ML and TF identified in the NRA. However, the relatively recent development of risk understanding at a national level by authorities is yet to translate into national AML/CFT policies consistent with the risks identified.

33. A project under the SRSP[7] has been launched in 2020 aimed at enhancing the capacity of the competent Bulgarian institutions to effectively mitigate the risks of ML and TF and to update the NRA. The progress in this field is also monitored under the EU Semester cycle and the policy measures are addressing the 2019 and the 2020 EU Council's specific recommendations.

34. AFCOS Council (with the participation of the FID-SANS as a member) is involved in the regular meetings of the Interagency Working Group for elaboration of National Strategy for prevention and fight against irregularities and fraud affecting the EU's financial interests for the period 2021-2027.

1.4.2. Legal & institutional framework

Legal framework

35. The Law on the Measures Against Money Laundering (LMML), Law on the Measures Against the Financing of Terrorism (LMFT) and other legal acts were further amended in 2019 for the purpose of transposition of the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of ML/TF and amending Directives 2009/138/EC and 2013/36/EU (5th AMLD). The national legal framework for ML/TF is further complemented by different provisions of sectoral laws, providing for the functions and powers of supervisory authorities and licensing and registration requirements for FIs and DNFBPs.

36. The criminal investigation of ML, TF and associated predicate offences and the powers and functions of the Prosecution and the investigative authorities are regulated in the Criminal Procedure Code (CPC), Law on Special Intelligence Means (LSIM), European Investigation Order Act (EIOA), Extradition Act and European Arrest Warrant (EAEAW), etc., while the criminalization of ML, TF and associated predicate offences is introduced in the Criminal Code (CC). Regarding securing of assets and confiscation, the CPC and the Law on recognition, execution and enactment of acts for securing property (LREEASP) are applied.

37. The Non-Profit Legal Entities Act (NPLEA) provides for the existence of the non-profit legal entities (NPOs). There are other specific laws that settle other types of legal entities and arrangements (for example, the Cooperatives Act (CoopA) settles the creation and the existence of the cooperatives as legal form).

38. Due to the EU membership, EU regulations are directly applicable in Bulgaria, including EU Regulation 881/2002 (and its successors); EU Council Regulation 2580/2001; EU Council

[7] Funded under the REGULATION (EU) 2017/825 of 17 May 2017 on the establishment of the Structural Reform Support Programme for the period 2017 to 2020 and amending Regulations (EU) No 1303/2013 and (EU) No 1305/2013, as amended by Regulation (EU) 2018/1671 of 23 October 2018.

Common Position 2001/931/CFSP; Council Decision (CFSP) 2016/849; Regulation (EU) 2017/1509; EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862; Commission Regulation (EU) No. 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No. 920/2010 and No 1193/2011. These EU acts are further complemented by national legal provisions, e.g. through introducing sanctions for non-compliance, designation of competent authorities, etc.

Institutional framework

39. The main agencies involved in Bulgaria's institutional framework are the following:

- The **Financial Intelligence Directorate of State Agency for National Security (FID-SANS)** is an FIU of administrative type. FID-SANS receives, stores, analyses and disseminates information gathered as per the LMML, LMTF and the Law on the State Agency for National Security (LSANS). FID-SANS plays an active role in development of AML/CFT policy in Bulgaria. Representatives of the FID-SANS are involved in various working groups and projects including for the development of AML/CFT legislation and leading the process of conducting the National Risk Assessment. Besides its functions as FIU of Bulgaria, the FID-SANS is also the AML/CFT supervisor over the activities of the obliged entities under the LMML. In this capacity, FID-SANS exercises control over the implementation of LMML and LMTF. Part of the supervisory functions of the FID-SANS is shared with Bulgarian National Bank, Financial Supervision Commission and National Revenue Agency.

- The **Bulgarian National Bank (BNB)** is the licensing authority for banks, payment institutions (PIs) and electronic money institutions (EMIs) and registration authority for other FIs under the Art.3a of the Law Credit Institutions (LCI). The BNB is the AML/CFT supervisory authority for banks operating in the territory of Bulgaria, including branches of banks from third countries, as well as branches of banks authorised by other Member States. The BNB performs similar controls regarding PIs and EMIs, including those that act through representatives in the territory of Bulgaria, as well as branches of PIs and EMIs authorised by other Member States.

- The **Financial Supervision Commission (FSC)** is the licensing authority for entities operating in the securities sector and insurance sector. The FSC is also the AML/CFT supervisory authority for securities and insurance sector.

- The **National Revenue Authority (NaRA)** is responsible at the national level for licensing and supervision of the entities operating in the gambling sector (land based and remote casinos). Although in practice the NaRA also fulfills some AML/CFT supervisory duties over the currency exchange offices, the legal basis for this is not explicitly established.

- The **Communications Regulation Commission (CRC)** is responsible for licensing of postal service operators than conduct postal money orders (PMOs). Although in practice the CRC fulfills some AML/CFT supervisory duties, the legal basis for supervision is not explicitly established.

- The **State Agency for National Security (SANS)** and its specialized directorates perform functions of surveillance, detection, counteraction and prevention of encroachments against national security, whether plotted, prepared or perpetrated. These activities include, among others, the defense of financial security (performed by the respective specialized directorate FSD-SANS) as well as the detection, prevention and disruption of attempts for terrorist activities and

terrorism financing and facilitation in Bulgaria (performed by the counter-terrorist specialized directorate CTD-SANS).

- The **National Counter Terrorism Centre (NCTC)** has the leading coordination role in countering terrorism and TF, located within the State Agency for National Security. NCTC is a unified national platform for coordinating the activities of competent Bulgarian authorities in the field of countering terrorism, violent extremism and radicalization, including by gathering and processing of information aimed at indentifying individuals and organizations related to terrorism. NCTC provides information necessary for exposing, countering and neutralizing terrorist threats, in a continious 24/7 regime to all reactive structures from the security and public order sector in the country. NCTC is aimed at supporting the coordinated management of national resources in order to raise the effectiveness of the national system for countering terrorism.

- The **Ministry of Interior (MoI)** is charged with national security and the upholding of law and order in the country. It undertakes operative and investigative work, to counter crime and national security threats and to maintain public order. The MoI is comprised of several general directorates including General Directorate "National Police" and General Directorate "Combating Organized Crime" the responsibilities of which involve investigations of money laundering, terrorism financing and related predicate crimes.

- The **International Operational Co-operation Directorate** is a structure of the MoI responsible for the organisation and co-ordination of the international exchange of operational information, for co-ordination and guidance of the international operational co-operation and for carrying out extradition, delivery and transfer of persons (Art. 43a, para 3 of the Ministry of Interior Act). The International National Operational Co-operation Directorate is the national contact point in the context of the International Criminal Police Organisation (INTERPOL), of the European Union Agency for Law Enforcement Cooperation (EUROPOL), of the European Travel Information and Authorization System (ETIAS) and the Schengen Information System (SIS) and shall perform the undertakings of the Republic of Bulgaria as National Central Bureau Interpol, Europol National Unit, ETIAS National Unit and SIRENE Bureau.

- The **Prosecutor's Office of the Republic of Bulgaria** directs the investigation of committed crimes and supervises the legality of the whole investigative process; brings accusation to criminals and maintains the accusation in criminal cases of general nature before the court, as well as exercises supervision over the execution of the criminal and other coercive measures. The Prosecutor's Office (PO) is headed by a Prosecutor General and its structure consists of 28 district territorial POs, which are competent to hear ML cases, with the exception of ML cases led by the Specialized Criminal Court. There are investigation departments at the territorial and specialized POs, Investigators are magistrates who, under the direction of the prosecutor, conduct investigations on certain, usually complex cases. Since 2017, the Specialized Prosecutor's Office (SPO) has been handling cases of corruption and corruption-related crimes including ML committed by certain officials of the legislature, the executive and the judiciary, as well as TF cases and investigations connected with criminal associations aimed at ML/TF. Supervision over the acts and actions of the district and the specialized prosecutor's offices is carried out by the appellate (5 territorial and 1 specialized) prosecutor's offices and by the

Supreme Cassation Prosecutor's Office.[8]

- The **Commission for Anti-Corruption and Illegal Assets Forfeiture (CACIAF)** is a standing independent specialized body established in accordance with the Law for Combating Corruption and Illegal Assets Forfeiture (LCCIAF). It is the legal successor of the Commission for Illegal Assets Forfeiture (CIAF). CACIAF presents an annual report on its activities to the National Assembly. The main task of CACIAF is to pursue the policy of combating corruption and illegal assets forfeiture.

- The **Ministry of Foreign Affairs (MFA)** is the competent authority which manages coordinates and controls the execution of the foreign policy and international activities of the Republic of Bulgaria. MFA coordinates international cooperation and participates in the drafting, signing and implementation of international treaties by the State. In this regard, at national level, the competent authority with responsibility to propose persons or entities to the relevant UN Committees is the MFA, given its vested powers as the national coordination authority on issues pertaining to the imposition of UN sanctions.

- The **Directorate "UN and cooperation for development" of MFA** analyses and keeps track for the fulfilment of the resolutions of UNSCRs related to preservation of international peace and security, incl. the imposition of sanctions, and undertake measures at national level for implementation of the sanctioning regimes.

- The **Ministry of Finance (MoF)** has a Regulation of Financial Markets Department that is responsible for the drafting and consultation of legislation in the field of financial markets and financial services. This Department consults also draft legislation in the area of AML/CFT measures. The Ministry of Finance participates in the Working Groups established to deal with AML/CFT issues. Representatives of the Ministry took part in the WG for the harmonisation of the 4th and 5th AML Directives of the EU that were established with joint order of the Minister of interior and the Chairperson of SANS. Representatives from the Ministry of Finance participate also in the WG that drafted and consulted the 2019 National Risk Assessment and are members of the permanent NRAM WG that was established through Council of Ministers Decision № 314 from 30.05.2019 amended with Decision № 523 from 02.09.2019.

- The **National Customs Agency (NCA)** is a centralised administrative structure within the Ministry of Finance. The directorates general and the directorates in Central Customs Directorate within their competence analyse, prognosticate and offer solutions and measures for uniform application of the EU law and of the national legislation in view of increase in the budget revenue, ensuring safety and security of citizens, protection of the EU financial interests and the national financial interests, protection from unfair and illegal trade and facilitation of legitimate trade. With regards to its competences related to cash controls and controls on the international commerce, National Customs Agency participated in the drafting of the ML/TF NRA and is part of

[8] Bulgaria has disbanded the Specialized Prosecutor's Office, as well as the Appellate Specialized Prosecutor's Office, the Specialized Criminal Court and the Appellate Specialized Criminal Court by virtue of the Law on Amendments and Supplements to the Judicial System Act (adopted on 14 April 2022 and published in No. 32 of the State Gazette on 26 April 2022). According to this draft legislation, the pending cases will be transferred to ordinary POs and courts, while the specialised judges, prosecutors and investigators will have an opportunity to apply for positions to be opened at the same ordinary POs and courts. Since this change took place after the onsite, it cannot be taken into account for assessment or rating purposes.

the permanent NRAM working group.

- The **Ministry of Justice (MoJ)** is a central authority concerning all the various types of international legal assistance, including mutual legal assistance requests, transfer of proceedings, transfer of sentenced persons, extraditions, recognition and enforcement of judgements, etc. The latter and the specific competences as central authority, terms within which the Ministry should act, are provided for in Chapter thirty-six "Proceedings in relation to international cooperation in criminal matters" of the CPC. There is a special department "Legal Cooperation in Criminal Matters" within the Ministry of Justice, executing the functions of the MoJ as central authority for international legal cooperation. Depending on the type of the act requested and the stage of criminal proceedings (pre-trial or court stage), the MoJ refers the request either to the Supreme Prosecution Office of Cassation or to the competent court for execution (which are the competent bodies for execution of the requests).

- The **Registry Agency within the MoJ** administers the property register, the BULSTAT Register, the Commercial register and the Register of property relations of the spouses. Basic and beneficial ownership information for legal persons and other legal entities registered on the territory of the Republic of Bulgaria is entered and available in the BULSTAT Register and the Commercial register

1.4.3. Financial sector, DNFBPs and VASPs

40. An overview of the financial and non-financial sector is provided in the table below. Detailed information regarding PMO, alternative investments, VASPs and DNFBPs except online gambling is not available.

Table 1.1: Overview of the financial and non-financial sector

Type of entity	**No.[9] Licensed/ Regulated/ Registered**	**Size of sector[10] (EUR)**
FINANCIAL SECTOR		
Banks[11]	18	63.53 billion (total assets)[12]
Branches of foreign banks	7	2.15 billion (total assets)
Payment institutions (PIs)	5	55 million (total value of outward transactions)
E-money institutions (EMIs)	8	10.1 billion (total value of outward transactions)

[9] As at 31 July 2021
[10] Data of 2020
[11] Banking sector is dominated by EU bank subsidiaries and EU bank branches (approx. 71,5 % of the total banking sector assets), followed by domestic banks (approx. 24,4 %); assets of non-EU banks and branches amount to 3,1 % of the total banking sector assets.
[12] https://www.bnb.bg/bnbweb/groups/public/documents/bnb_publication/pub_b_in_b_2021_06_en.pdf

Postal money order providers (PMOs)	37[13] PMOs, 9157 branches	No information provided on value of transactions[14]
Asset management companies	29 and 1 foreign branch	295 million (total assets)
Investment firms (non-banking)	35	9.96 million (total assets)
Banks (providing investment services)	17	17.07 million (total assets)
Alternative Investment Fund Managers	15	67 million (total assets)
Alternative investment funds	17	No information provided
Collective investment schemes	125	1.1 million (total assets)
Insurance companies	10	71.44 million (Total value of premiums relating to investment linked insurance)
Insurance/reinsurance brokers	208	1.6 million (Total value of premiums relating to investment linked insurance)
Currency exchange offices	2455	4.06 billion (total value of transactions)
VASPs	26	Not available[15]
Financial leasing companies	44	1.98 billion (total value of assets)
Lending (incl. factoring) companies	151	1.91 billion (total value of assets)
Other FIs	7	126 million (total value of assets)
NON-FINANCIAL SECTOR		
Casinos	20	No information provided
Online gambling operators	12	5,8 billion (Total amount of bets) 5,65 billion (Total amount of winnings)
Notaries	719	n/a
Lawyers	13605	n/a

[13] Of which 19 PMOs with 2546 branches were not active in 2020. Branches in this context should be understood as client service locations.

[14] Only number domestic and cross border transactions available which cannot be considered size indicator.

[15] VASPs become subject to regulation at the end of 2020.

Law firms	1116	n/a
Accountants	Not available	n/a
Real estate agents	Not available	n/a

41. The AT has ranked the sectors on the basis of their relative importance in Bulgaria given their respective materiality, the most significant features of the FIs/DNFBPs sectors, nature and scale of their activities, ML/TF vulnerabilities (including deriving from regulatory environment) and the level of ML/TF risks exposure. The materiality related considerations are applied throughout the report, with a deeper focus at IO.3 and IO.4.

42. **The banking sector** was weighted the most heavily based on its materiality and risk exposure. The banking sector offers the broadest range of the financial services to the largest proportion of the various types of clients, including non-residents, etc. The NRA identified the banking sector as one of the sectors under the highest threat of being abused for ML; it is ranked in a leading position by the law enforcement authorities and the financial intelligence services among the most frequently used channels for money laundering. Incoming and outgoing banking transfers represent the most commonly used banking products in actual and suspected ML schemes. Such transfers are usually carried out between legal persons at the ML layering stage and include forged documentation to justify the transactions.

43. **Money value transfer service business sector** is the second in terms of priority. In 2020 total values of outward money remittances totaled BGN 10.197 billion (approx. EUR 5.2 billion)[16]. Revenues from postal money orders alone represent 0,013% of GDP[17] (approx. EUR 8 million). Money remittance services that can be provided by the banks, payment institutions, e-money institutions and postal remittance providers, as well as the branches and agents of the foreign owned providers, carry the risk of both ML and TF, especially considering the geographical location of Bulgaria and the related vulnerabilities (migrant community, close proximity to Balkan countries and conflict zones, operation of hawala network). Serious shortcomings in the licensing and supervisory regime of postal remittance providers makes the sector even more vulnerable to ML/TF abuse.

44. **Real estate agents (and notaries attached to the real estate deals)** are the highest weighted DNFBP sector. Real estate agents and notaries are significantly exposed to ML risks due to the sectorial vulnerabilities, namely, no registration and licensing regime and relatively weak supervision of the real estate agents; and due to the prevalent use of real estate deals to disguise criminal origin of funds, as well as cases of real estate price manipulations.

45. **Lawyers and accountants** that provide company formation and other activities covered by the FATF standard[18] are the second highest weighted DNFBP sectors. Lawyers and accountants

[16] According to data under Regulation (EU) № 1409/2013 of the European Central Bank on payments statistics.

[17] The total revenues for money remittances and, conversely, the total value of PMO remittances has not been provided to the AT.

[18] See c.21.1, sub-criterions (d) and (e).

are weighted heavily due to their gatekeeping role which is critical in light of the prevalent use of Bulgarian established companies in money laundering schemes. This, combined with the vulnerabilities of the regulatory regime (there is no separate registration/licensing regime for trust and company service providers (TCSPs) and no registration regime for accountants), lead the AT heavily weight lawyers and accountants.

46. The **providers of currency exchange** and **VASPs** are weighted third in terms of priority. The large size of the currency exchange sector (nearly 2,5 thousand entities), combined with the cash related risks exposure and the criminogenic situation in the country, as well as the vulnerabilities related to regulatory and supervisory framework attributed to the significant weight given to the currency exchange sector.

47. **VASPs**' relatively high materiality is determined by the lack of available data regarding nature and scale of activities as well as the vulnerabilities of the regulatory and supervisory regime: (1) no controls to prevent criminals and their associates from entering the market; (2) regulatory regime has been introduced at the end of 2020 and (3) supervision is at the infancy stage; and cases of unregulated Bulgarian VASPs featuring in fraud and ML schemes, according to public sources.

48. **The other sectors that are rated moderately important** are securities and gambling operators. Although securities are rated in the NRA as relatively high risk, this was mainly due to the prevalent cases of abuse for fraud[19] purposes and remote identification. Gambling is moderately weighted primarily due to the issues surrounding the former regulator.

49. **Less important sectors are** insurance and other types of financial institutions such as credit co-operatives, leasing and lending due to lower inherent vulnerabilities and smaller size/scale of activities. Throughout the report, reference to insurance means both the social (pension) insurance and the general insurance sectors, i.e., life insurance and other investment related insurance (e.g., pension schemes).

1.4.4. Preventive measures

50. The preventive measures are set out in two main laws governing AML/CFT regime in Bulgaria, namely – LMML and LMTF – where LMML governs AML matters and LMFT governs TF and targeted financial sanctions (TFS) related to TF matters.

51. The regulatory, i.e., licensing and supervisory regime, does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except when they are provided by banks) and certain VASP activities, namely: persons providing exchange between one or more forms of virtual assets; transfer of virtual assets; participation and provision of financial services related to an issuer's offer and/or sale of a virtual asset. The dealers of precious metals and stones are not subject to preventive measures following the prohibition from conducting transactions in cash that exceeds BGN 10 000 (approx. €5 000).

52. DPMS are exempted from the AML/CFT requirements following the introduction of cash transaction threshold over € 5 000.

53. The AML/CFT requirements extend to certain activities which are not covered by the FATF standard, e.g., auditors, bailiffs.

[19] Majority of fraud cases are not attributed to the regulated sector.

1.4.5. Legal persons and arrangements

54. The Bulgarian legal framework provides for the establishment of the following types of legal persons: General partnership; Limited partnership; Limited liability company; Sole-owned limited liability company; Joint stock company; Sole-owned joint stock company; Special investment purpose company; Limited stock partnership; Cooperatives; State Undertakings; Public Undertaking Merchants; European economic interest grouping (EEIG); European Cooperative Society; European Company (Societas Europaea); Companies registered in preferential tax regime jurisdictions; Branch of a foreign legal entity; Association; Foundation; Branch of foreign NPO; Community Culture Center.

55. Other legal forms include: (1) legal persons established under the National Community Centers Act or specialized national administrations and agencies established by a special normative deed (e.g., the National Agency for the State reserve and war time supplies established under the State Reserve and War time Supplies Act); (2) Certain other legal entities (which are established as JSCs or LLCs) which carry out a national function or are owned (in majority or in full) by the State are established by special legal acts (such as the Medical Establishments Act, the Public Enterprises Act, etc.) and these acts provide additional requirements as to their establishment, existence, directors, etc. The following forms – Association, Foundation, Branch of foreign NPO, Community Culture Center – are referred to as NPOs.

56. Bulgaria describes the types, forms and basic features of legal persons in a variety of different pieces of legislation. The vast majority of legal forms in Bulgaria are Companies (Commerce Act (CA)), Non-Profit Legal Entities (Non-Profit Legal Entities Act (NPLEA)), Cooperatives (Cooperatives Act (CoopA).

57. Bulgarian domestic law does not provide for the existence of trusts, however, the professional trustees administering foreign trusts and other similar types of legal arrangements formed under the foreign laws can exist in Bulgaria. In those circumstances they are legally required to provide BO information to the BULSTAT Register. However, currently there is little awareness of this phenomenon and no data available to determine the risks posed thereby.

58. NRA findings indicate that the limited liability companies (LLC) especially those using informal nominees (strawmen) or establishing complex corporate structures (including owned/managed by offshore companies or legal arrangements administered in other jurisdictions) to disguise ownership are often used for ML purposes in Bulgaria.

59. In March 2018 the new LMML introduced specific requirements for the provision, entering, availability and access to data on beneficial owners of the legal entities and legal arrangements in the respective centralised databases – the Commercial Register, BULSTAT and the Register on non-profit organisations. The registers currently provide an opportunity for the obliged entities and competent authorities to conduct checks in it.

60. Basic and beneficial ownership information on the legal persons and arrangements is administered by the **Registry Agency within the MoJ**.

Table 1.2: Numbers of legal persons registered in Bulgaria (as of 31 July 2021)

Type of Legal Persons / Arrangements	Number
General partnership	6171
Limited partnership	101
Limited liability company	186842
Sole-owned limited liability company	578767
Joint stock company	9431
Sole-owned joint stock company	3369
Special investment purpose companies	67
Limited stock partnership	27
Cooperative	3517
State Undertakings	18
Public Undertaking Merchant	3
European economic interest grouping (EEIG)	18
European Cooperative Society	1
European Company (Societas Europaea)	3
Companies registered in preferential tax regime jurisdictions	40
Branch of a foreign legal entity	604
Association	15378
Foundation	2917
Branch of foreign NPO	110
Community Culture Center	2642

1.4.6. Supervisory arrangements

61. Financial institutions. The BNB is the licensing authority regarding credit institutions, payment and e-money institutions and manages a public register of others FIs (financial leasing, guarantees, factoring, forfeiting). The FSC is the licensing authority regarding securities and insurance, the CRC is the licensing authority regarding postal operators and the NaRA manages a public register of currency exchange offices.

62. DNFBPs. The NaRA is the licensing authority regarding gambling; lawyers are registered by the Bar Association, Notaries are registered by the notary Chamber of Bulgaria and auditors by the Commission for Public Oversight over Registered Auditors. Accountants, real estate agents and trust and company services providers (TCSPs) are not subjected to licensing or registration.

63. Regarding AML/CFT supervision, the FID-SANS is designated as the control authority responsible for ensuring OEs compliance with the AML requirements (Art. 108(2), LMML) and with CTF and TFS related to TF requirements (Art. 9A(2), LMFT). Further, control of compliance with the requirements may also exercised - either independently or jointly with the FID-SANS - by the BNB (regarding credit institutions, payment and e-money institutions), FSC (regarding securities and insurance) and NaRA (regarding gambling); this includes both, on-site and off-site supervision (Art. 108(6), LMML). The LMML provides for the possibility to carry out joint inspections (between FID-SANS and the above-mentioned authorities). Although in practice the NaRA is tasked with supervision regarding currency exchange and the CRC regarding postal operators, the legal basis for this supervision has not been established (see R.27).

64. Although legally appointed supervisors have powers to compel information regarding compliance with the LMML, the powers to compel information related to compliance with LMFT (on TF and TFS related to TF) is granted only to the FID-SANS and BNB (see R.27).

65. There is no established legal basis to supervise implementation of TFS related to PF.

1.4.7. International cooperation

66. The importance of international cooperation in criminal matters for Bulgaria stems from the geographical location of Bulgaria and the country's ML/TF risk profile. Factors particularly relevant in this field include criminal ML offences related to foreign proceeds where there is a need to prove the criminal origin of the assets abroad as well as the prevalence of predicate offences committed in an essentially trans-national manner, mainly due to the fact that Bulgaria is a part of the Balkan route. The mentioned exposes the country to, e.g., illegal trafficking and trade in drugs, people, arms and both licit and illicit goods particularly by organised crime groups, and other crimes with international nexus. With respect to ML/TF issues the most significant international partners for Bulgaria are the member states of the EU and neighbouring jurisdictions.

67. The Bulgarian legislation sets out a comprehensive legal framework for international cooperation in criminal matters, which enables the authorities to provide a broad range of assistance concerning ML/TF and associated predicate offences. Assistance is provided on the basis of various legal arrangements and international instruments. These include UN, Council of Europe Conventions and EU legal instruments, treaties and other bilateral agreements on MLA in criminal matters and extraditions, as well as EU Framework Decisions. The MoJ serves as the central authority for international cooperation in MLA requests in the trial stage in Bulgaria. In the pre-trial stage foreign MLAs (including European Investigative Orders (EIOs)) are executed by prosecutors, where central authority is the General Prosecutors Office (EIOs are sent directly to competent Prosecutors Office and cases involving OCG to Sofia City Prosecutors Office). In cases of criminal proceedings channels of cooperation through direct communication are used by the MoI (police) and the FID-SANS with respective foreign partners.

2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

a) Bulgaria completed its first holistic NRA in 2019 using a methodology designed by the CoE. Overall, the authorities demonstrated a reasonable level of understanding of the main ML risks Bulgaria faces. ML threats are well analysed, however, the analysis of the vulnerabilities is not yet sufficiently developed meaning that the analysis of residual risk is limited. In some areas, there has been a reasonable analysis of the risks arising from various predicate offences (such as organised crime and tax crimes). In other areas, understanding is hampered by lack of detailed consideration of the significant risks related to certain major predicate offences (such as corruption). There is also limited understanding around the use of domestic and foreign legal entities for obscuring beneficial ownership and involvement of lawyers, accountants and notaries in the facilitating the ML.

b) Understanding on ML risks significantly varies authority to authority; FID-SANS, the BNB and the FSC demonstrated fair understanding of the risks whereas other authorities demonstrated a more limited understanding with some critical authorities such as the prosecution authorities and agencies with responsibility for anti-corruption occasionally demonstrating a very limited understanding.

c) TF risk in Bulgaria is understood to a limited extent by all authorities. It is currently limited to having a basic understanding of the cash economy in Bulgaria by the authorities and a developing understanding of how its geographical position may influence TF risk. Whilst some initial analysis has been conducted concerning the incoming and outgoing financial transfers, it has not yet been used to develop understanding of risk (particularly for high-risk countries) or used to develop appropriate ML/TF policies. Bulgaria has not conducted a proper and thorough TF risk assessment of its NPO sector.

d) Bulgaria has recently adopted an Action Plan which looks to address the risks identified in the NRA exercise. This includes an outline of priority levels, responsible authority, deadline and resources and fiscal implications. Several actions are already underway, with some having made significant progress (notably in key risk areas such as real estate). However, whilst a very limited number of competent authorities have focussed on areas identified as higher risks in the NRA, overall, the objectives and activities of the competent authorities are not yet consistent with the ML/TF risks identified.

e) The work in the Action Plan demonstrates the extent to which development of risk understanding has only very recently started to translate into national AML/CFT policies. However, the lack of a National Strategy under which such policies can be developed is a significant shortcoming.

f) Bulgaria faces major issues concerning co-operation at a strategic level in developing risk understanding and implementing appropriate policies to mitigate ML/TF). The NRAM WG has been designated to continue the work of the NRA by the creation of the AML/CFT Action Plan and future co-ordination of ML/TF policies, however, authorities resource issues remain to deliver over 50 high level actions. Risk understanding and co-ordination work is also hampered by the lack of suitable technology systems which can work on a multi-agency basis and lack of meaningful statistics in certain areas.

g) At an operational level, major issues exist in co-operation between authorities with a concern of duplication of the supervisory efforts for some sectors and lack of supervision for other sectors (including high-risk sectors). Concerns remain about the overly formal approach to national cooperation, which can delay the timeliness of international cooperation.

h) The private sector has a general awareness of the NRA and its conclusions, however, engagement by the country with the private sector has been relatively minimal, therefore limiting their detailed understanding of ML/TF risk. More recently, and post the conclusion of the NRA, the authorities have moderately increased outreach to NPOs, FIs and DNFBPs regarding NPO TF risks.

i) Authorities understand potential for abuse of the investment-related residence and citizenship (IRRC) programme by non-resident natural persons and how it can be abused for ML. The particular exposure of the IRRC to the laundering of corruption funds is acknowledged and understood. However, this understanding has not yet translated into appropriate policies to prevent against abuse of the IRRC.

j) The NRA process covers generally the activities of VASPs and the potential misuse of legal persons for ML, however, Bulgaria is yet to comprehensively conduct a risk assessment of these areas. Given the nascent nature of risk understanding in this area, it is not possible to say that authorities yet have a comprehensive understanding of risks that VASPs pose to Bulgaria.

k) Bulgaria has basic understanding on ML/TF risks that the informal economy presents and limited measures to address ML/TF risks that the informal economy presents to Bulgaria.

l) Not all activities that are covered by the FATF definitions for FI and VASP are subject to preventive measures in Bulgaria.

Recommended Actions

a) Bulgaria should translate its ML and TF risk understanding into national AML/CFT policies under the umbrella of a national AML/CFT strategy (a long-term strategic document). This should include the ongoing work under the Action Plan (which represents a short/medium term working document) and this programme of work should look to mitigate the risks identified in the NRA. In conducting this work, the objectives, activities and resources of the competent authorities (particularly concerning prioritisation of activity) should be consistent with an ongoing understanding of the ML/TF risks in Bulgaria.

b) In order to ensure that appropriate co-ordination of national policies and measures can occur, the authorities should urgently review NRAM WG's proper status, structure, and resources to ensure its ability to:

   i. co-ordinate the development and implementation of policies[20]and activities to combat ML/TF and PF effectively and holistically for all competent authorities

   ii. implement the NRA Action Plan effectively, according to the set deadlines

   iii. to undertake significant further risk assessment work in Bulgaria.

c) Bulgaria should establish comprehensive national inter-agency information exchange channels to avoid the overly formal national cooperation, which can delay the timeliness of international cooperation.

d) With regard to understanding of ML/TF risks, Bulgaria should ensure there are sufficient resources for the FID-SANS and other authorities to develop ongoing risk understanding (particularly on new/emerging risks) and notably to keep the NRA up to date and enhance the risk assessment work. Additional risk assessment work should include:

   i. further analysis of the ML risks with a greater focus on the vulnerabilities in key sectors (see IO.3 and IO.4 for key sectors). This should look to produce a more accurate analysis of residual risk which can inform policy and strategy development in Bulgaria

   ii. further analysis regarding the significant risks connected with a number of major predicate offences, notably corruption, the use of domestic and foreign legal entities for obscuring beneficial ownership, the involvement of lawyers, accountants and notaries in facilitating ML and the potential abuse of citizenship investment schemes to obtain citizenship through investment with laundered funds.

e) In respect of TF risk assessment, Bulgaria should look to utilise information on incoming and outgoing financial transfers across all authorities (particularly considering high-risk countries) to further develop its understanding of TF risk at a national level. This analysis should be used to develop risk-based policy decisions and operational responses to TF risk, especially supervisory actions.

f) Bulgaria should review the operation of the IRRC, with a specific focus on the ML risks that it presents and look to adopt appropriate policies and measures to prevent abuse of the IRRC.

g) Bulgaria should develop more effective data collection tools or mechanism in order to collect sufficient statistics that would support conducting NRA updates and performing strategic analysis with minimum of having better statistics on:

   i. STRs (breakdown of predicate offences indicated in STRs) (see IO.6)

[20] Having regard to AML/CFT requirements and Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation) as needed.

ii. investigations, prosecutions and convictions on ML offences, related predicate offences (see IO.7)

iii. seizures, freezing and confiscations and respective criminal offences (see IO.8)

iv. in- and outgoing MLA requests on seeking and providing MLA and other forms of international cooperation for AML/CFT purposes and related predicate offences (see IO.2).

h) Bulgarian authorities should conduct significantly more engagement with the private sector (particularly those sectors identified at being most at risk of being abused for ML) to raise awareness of the conclusions of the NRA. Supervisors (particularly the FID-SANS) should also significantly enhance how their engagement develops risk understanding in the industry.

i) Bulgaria should look to conduct further risk assessment on the informal economy and consider whether further policies (building on existing good policies, such as cash limits) should be introduced to continue to mitigate the significant ML/TF risk that the informal economy presents to Bulgaria.

j) Bulgaria should conduct a proper and thorough TF risk assessment of its NPO sector and communicate the results to NPO, FI and DNFBP sectors.

k) Bulgaria should identify and assess the ML/TF risks emerging from virtual asset activities and the activities or operations of VASPs.

l) The authorities should extend the scope of the LMML to apply to all activities covered by FATF definitions for FI and VASPs.

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

2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1. Country's understanding of its ML/TF risks

69. Bulgaria completed its first holistic NRA of ML and TF risks in 2019 using methodology designed by the Council of Europe (CoE).[21] The NRA was based on statistics taken from between 2013 - 2016, along with questionnaires sent to the private sector and analysis by working groups in 2017 - 2018. The NRA was led by an NRAM WG established by joint Ministerial Ordinance.

70. This NRA is a product of consultation across government, law enforcement, intelligence agencies, supervisors, and the private sector. Sources used include public national and

[21] The NRA is not the first document attempting to measure ML/TF risks in Bulgaria. In 2012 a pilot project led by the International Monetary Fund (IMF) was finalised. This preliminary risk assessment was conducted by applying methodology developed by the IMF. The key findings of this preliminary assessment showed that large amounts of money laundered originate from committed domestic VAT fraud (NRA, p.13).

international reports in the relevant areas, including from Europol, the FATF, MONEYVAL and the EU Supranational Risk Assessment of ML and TF (SNRA).

71. The NRAM WG and ad-hoc WG were co-chaired by the SANS (through the Head of the FIU) and the Ministry of the Interior (through the Head of the AML Unit of the General Directorate, Combatting Organised Crime). After the adoption of the new LMML, as envisaged by Art. 96 of the law, a permanent interdepartmental NRAM WG was established through a CoM Decision that is a successor of the ad-hoc WG. The NRAM WG contains members from authorities in Bulgaria who are relevant to combatting ML/TF. The NRAM WG also acts as the only co-ordinating body for risk assessment and ML/TF policy work across all agencies in Bulgaria.

72. The authorities, and particularly the FID-SANS, should be commended for the significant work that has occurred in undertaking the NRA process and producing a comprehensive report. Risk factors were examined using data available to authorities that has been subject to analysis across authorities and the private sector.

73. The FID-SANS is the key agency in relation to risk assessment work and it is critical that is has the correct level of status in the country along with sufficient resources to continue risk assessment work at a suitable level. Pursuant to the LMML, the NRA shall be up-dated every two years – with the next NRA scheduled for 2020 - 2021. At the time of the onsite authorities were still in the process of updating the NRA.[22]

74. The NRA was based on a reasonable analysis of risks based on the following components: analysis of threats, based on the case studies, stemming from predicate criminality, which serves as the main source for generating criminal proceeds; analysis of subjects undertaking ML; analysis of economic sectors associated with ML; analysis of financial/DNFBP sectors and products abused for ML and TF; cross-border characteristics of ML; and analysis of TF risks.

75. Statistics for analysis were generally taken from 2013 - 2016 but varied in comprehensiveness agency to agency. The lack of available comprehensive statistical data and a comprehensive mechanism by which to obtain relevant data on a national level is a significant impediment to risk assessment in Bulgaria (see also IOs 2, 6, 7 and 8). Equally, the fact that much of the data is taken from before 2016 brings into question how up to date the report can be considered.

76. The AT consider that the NRA Report and process demonstrates a reasonable general understanding across most authorities of the main ML risks that Bulgaria faces. The report contains a good initial analysis of the ML threats Bulgaria faces, however; generally, the analysis of the vulnerabilities is not yet sufficiently developed meaning that the analysis of residual risk is limited. Whilst some sectors such as the banking sector have a developing understanding of the vulnerabilities of the sector to ML/TF, this is not held across other sectors. The NRA also does not consider in sufficient detail the significant risks connected with a number of major predicate offences that require further detailed consideration – particularly the laundering of proceeds of corruption, the use of domestic and foreign legal entities for obscuring beneficial ownership, the involvement of lawyers, accountants and notaries in facilitating ML and the potential abuse of citizenship investment schemes to obtain citizenship through investment with laundered funds. The lack of detailed risk understanding in these areas inhibits the ability of Bulgaria to develop

[22] Covid-19 pandemic has impacted the process of updating the NRA to some extent.

national AML/CFT policies to mitigate these risks. This is both reflected in a lack of detailed analysis in the NRA report but also in the authorities more generally.

ML Risk

77. The CoE risk assessment methodology conducts an analysis of a variety of data sources to produce a series of risk events for a country.

78. Bulgaria identified eight of the top ML risk events as a result of the NRA: laundering of funds from a range of foreign and domestic predicate offences linked to organised crime (primarily drugs, human trafficking and tax evasion) through the exploitation of the formal financial system and extensive use of cash; laundering the proceeds of corruption (particularly noting property and misuse of EU funds) through complex domestic and foreign-based ML layering schemes with assistance of ML professionals; laundering of funds from tax evasion and VAT fraud using straw men; integration of funds in the construction and real estate sector; laundering of funds from foreign predicate offences through non-bank investment intermediaries; laundering of illicit funds generated in the food and oil trade (tax fraud and evasion) using shell companies and informal nominees; laundering of funds from computer and social engineering fraud; involvement of ML professionals and reporting entities (due to vulnerabilities in market entry and employee screening).

79. Inherent threat factors were generally well understood, noting that Bulgaria is part of an established trade and transportation corridor between the Middle East and Europe known as the '*Balkan Route'*. All authorities therefore had a good understanding as to how their geographical position contributed to ML risk and how it can affect a variety of financial and non-financial sectors. The transportation of large volumes of cash across the borders to and from Europe and how this increases ML risk was acknowledged.

80. Aggravating contextual factors such as how the large cash-based economy (constituting around 30% of GDP) along with the identified levels of corruption and potential issues with the effectiveness of certain authorities were also well understood as to their impact on overall ML risk. During the course of the on-site evaluation, discussions occurred regarding the understanding of risk in the informal economy. Apart from the issues associated with cash, and the associated policies, the Bulgarian authorities did not demonstrate a significant understanding of the informal economy and how it impacts the ML/TF risks in the country. There was limited consideration of any further policies to address this area of potential risk.

81. Overall, Bulgaria concluded that their greatest ML predicate offence risk was organised crime offences such as trafficking in human beings or narcotics, and the trade of contraband goods, such as cigarettes, alcohol, and fuel, as well as tax crimes and fraud (including computer and VAT fraud). The NRA also recognises that corruption as a ML predicate is also considered of major impact, however, the assessment of corruption risk in Bulgaria as a predicate to ML is impeded in the NRA exercise by lack of sufficient data and information. Generally, the financial elements related to corruption and other predicate offences has not been adequately examined by Bulgaria. There is also a more limited monitoring of PEP related transactions which limits risk understanding (as noted in IOs 4 and 6). Given the significant corruption risk in the country, this should be urgently addressed in specific detailed risk assessment.

82. The authorities demonstrated a reasonable understanding of the fact that "*ML professionals*" operate in Bulgaria both within organised crime groups and autonomously. The NRA process recognises that this lends itself to the abuse of complex legal structures both

domestically and abroad and the risk that legal and accounting professions could be involved in professional ML in Bulgaria.

83. The NRA recognises that both natural and legal persons are exposed to ML activity. It acknowledges that the use of straw men as a clear risk and notes that in respect of legal persons, the number of cases in Bulgaria are significantly higher than for natural persons.

84. A particular area of note is the potential for abuse of the investment-related residence and citizenship (IRRC) programme by non-resident natural persons and authorities appear to understand how it can be abused for ML. The particular exposure of the IRRC to the laundering of corruption funds is acknowledged and understood. However, the AT did not find evidence that this understanding had translated into any policies to prevent against abuse of the IRRC.

85. Risk understanding in relation to PEPs is generally well-understood and PEP related ML risks were regularly cited by authorities. However, the current level of risk understanding is also hampered by the availability of data in this area. PEP risk is acknowledged by all the authorities to be one of the highest risk factors in Bulgaria and the consequences of this leading to political and social destabilisation appear to be understood. This was an area where the private sector noted particular attention based on the ML risks, indicating understanding of ML risk in this area is reasonably well developed.

86. Generally, the significant use of cash is acknowledged as one of the major ML risks in Bulgaria. In the formal banking system, the greatest risk is understood as being linked to various types of incoming and outgoing transfers. All authorities noted that the banking sector is most vulnerable to being involved in ML relating to tax offences (including VAT related crimes) and fraud whereas in the securities sector the ML risk is significantly less but related to non-bank investment intermediaries running on-line trade platforms.

87. Authorities also acknowledged that MVTS is highly vulnerable to ML/TF in Bulgaria due to the large use of cash however, again, this significant vulnerability has not been addressed in any more detail by national policies outside of the 10 000 BGN cash transaction limit which has been in place for some time.

88. In respect of *DNFBPs,* most authorities have a good understanding of their exposure to significant ML risks, particularly where the activity relates to the real estate sector. The higher risk is understood by authorities based on the popularity of this sector amongst foreigners, the common use of the sector in ML integration and the low level of regulation. This has not been addressed by adequate policies that address these significant risks. To some extent, the involvement of lawyers and accountants in professional ML is also understood.

89. Authorities have a reasonable general understanding of the main ML/TF risks Bulgaria faces, but this varies from authority to authority. The FID-SANS, the BNB and the FSC demonstrated good knowledge whereas other authorities demonstrated a more limited understanding with some critical authorities such as the prosecution authorities and agencies with responsibility for anti-corruption occasionally demonstrating a very limited understanding.

90. Overall, considering the Risk Assessment and Ratings Matrix (part of the CoE Methodology) the AT take the view that given the significant number of high/extreme impact and consequence level of risk events in Bulgaria, risk understanding work and ML/TF policy work requires a significantly greater level of political priority in the country in order to deliver an effective AML/CFT regime.

91. The AT shares the view of Bulgaria as to the level of exposure of sectors to ML – however, at this stage risk understanding has not developed sufficiently to consider more accurately the vulnerabilities in specific higher risk sectors – using accurate and timely data.

92. In general, the BNB and FSC demonstrated fair understanding of ML risks in the banking sector which extends beyond the NRA. This has led to a comprehensive sectoral risk assessment in the banking sector published in 2021.

93. The sectoral risk assessment by the BNB has been developed from additional data collection from the banking sector and information taken from the BNBs supervisory activity and reports. The report takes into account the EU supranational money laundering and terrorist financing risk assessment and the NRA findings and produces a Vulnerability/Threat matrix identifying the level of risk related to various degrees of threat or vulnerability with regard to a specific product, service, segment or delivery channels. However, the BNB questionnaires don't include information on incoming/outgoing wires by country and questions remain on the process (see IO.3). The BNB have indicated this information will be collected in future questionnaires.

94. The FID-SANS demonstrated a reasonable understanding of ML risks which, in some areas, went beyond the NRA, while in other areas is limited due to absence of statistics and strategic analysis (see IO.6). There is a prioritisation matrix used by the FID-SANS which, in respect of the FIU, is a point of reference when prioritising their analysis of incoming STRs (see IO.6). However, prioritisation is not evident in the supervisory work of the FID-SANS and it is a significant shortcoming that the supervisory work of the FID-SANS is not based on ML/TF risk.

95. The LEAs and the prosecution authorities did not demonstrate any reasonable understanding of ML risk based on interviews and on many occasions appeared unable to articulate the conclusions of the NRA. In respect of some prosecution authorities and particularly the anti-corruption authorities, they occasionally demonstrating a very limited understanding. It appeared to the AT that for the anti-corruption authorities, it was unclear how their daily work was integrated with identifying ML and whether there was any reasonable understanding of the link between anti-corruption work and ML work in Bulgaria. Given the outcome of the NRA considering corruption risk in Bulgaria this is of significant concern to the AT.

TF Risk

96. The NRA process covered TF risk as well as ML risk – although the AT are of the opinion that the risk assessment process was not as comprehensive for TF as it was for ML and therefore the authorities understanding of TF risk in Bulgaria is more limited.

97. The NRA identifies the high-risk TF risk events in Bulgaria as follows: (i) use of MVTS and informal value transfer (*hawala*) to transfer funds potentially related to TF; and (ii) facilitation by migrant communities aggravated by large cash-based and informal economy. The NRA also notes that the potential diversion of funds allocated for NPO or religious activities in Bulgaria towards TF is of medium risk.

98. The authorities consider that TF activity in Bulgaria appears to be relatively restricted to the use of cash, money transfer services and the occasional use of illegal/informal financial services (hawala). Some TF risks have materialised in Bulgaria with regard to the existence of limited financial and material support for foreign organisations functioning abroad and the use of hawala system as a conduit for support. Equally, the authorities' analysis of NPOs reveal that an updated comprehensive analysis on the activities and vulnerabilities of NPOs is needed following the implementation of the largely redesigned NPO-related legal framework.

99. The TF risk assessment process and risk understanding generally by authorities in Bulgaria is impeded by a lack of data relating to financial flows and FIs/DNFBPs in Bulgaria. This is particularly notable when considering high-risk TF countries. Whilst the AT was provided with figures concerning financial flows data that was used in the NRA process, it is not clear that there has been adequate analysis of this information across authorities at a national level and it has not yet been used to develop understanding of risk (particularly for high-risk countries) or used to develop appropriate ML/TF policies. Whilst supervisors carry out some analysis of financial flow data in advance of supervisory visits, this is not sufficiently granular across all entities (particularly noting the significant risks in the MVTS sector) to result in meaningful risk understanding.

100. Bulgaria has a developing understanding of how its geography may influence TF risk in the country. The NRA report has separate chapter on cross-border risks that Bulgaria is facing which contains some analysis of geography of the money flow and the use of cash couriers acknowledging that Bulgaria has an external East and South border a (non-EU) and the risk of ML and TF through money flows from the neighbouring countries affected by complex geopolitical conflicts.

101. The AT therefore consider that TF risk is currently understood to a limited extent in Bulgaria.

VASP sector and misuse of legal persons

102. The NRA process covers generally the activities of VASPs and the potential misuse of legal persons for ML, however, Bulgaria is yet to comprehensively conduct a risk assessment of these areas.

103. In line with economic trends in other European countries, VASP activity is occurring in Bulgaria, and it is a growing sector. Authorities were not able to demonstrate any reasonable understanding of ML risks that VASPs presented, and they were not covered in the NRA due to the current lack of registration and licensing provisions and anonymity which has led to a lack of comprehensive data. A recent registration regime and a supervisor has been appointed for VASPs and the authorities indicated this will provide them with data on VASP activities in Bulgaria. However, as noted under R.15 and IO.3, the following deficiencies apply to the VASPs sector: (1) not all virtual assets related activities are covered by the Bulgarian legislation, i.e., persons providing exchange between one or more forms of virtual assets; transfer of virtual assets; participation and provision of financial services related to an issuer's offer and/or sale of a virtual asset are not treated as VASPs and thus are not subject to the AML/CFT requirements; (2) Bulgaria has no mechanisms in place to enforce registration of the persons that conduct VASPs activities, thus the entire population of VASPs has not been determined. Moreover, criminals and criminal associates are not prevented neither by legal nor regulatory measures to enter the VASP market (as a manager or beneficial owner of a VASP). The AT therefore considers that the authorities do not yet have a reasonable understanding as to ML/TF risks in the VASP sector nor have they taken any significant actions to mitigate any risks.

104. Whilst the NRA exercise generally covers the potential misuse of legal persons, this assessment is more general and does not consider in detail the ML/TF risks associated with each type of legal person created in Bulgaria. The analysis conducted by Bulgaria through the NRA exercise is high level and whilst it focusses on some risks associated with certain types of legal persons (LLCs) - notably in Chapter 4, it does not represent a comprehensive systematic risk assessment of the risks associated with all types of legal persons in Bulgaria. The analysis of the

inherent vulnerabilities of each relevant type of legal entity is currently not complete and the current analysis is very much driven by recent operational activity and does not adequately cover all entities and their exposure to Risk in Bulgaria. The NRA notes the particular risk of "*straw men*" being used in Bulgaria as well as the use of complex structures for ML. It is of particular note that nominee shareholders are not explicitly prohibited in Bulgaria meaning they can still be misused in this manner.

105. Whilst Bulgaria has taken some mitigating actions to prevent misuse of legal persons by prohibiting bearer shares and enhancing BO transparency by creating BO registry, the AT considers that there have been fundamental issues with implementation of these measures (for more information see IO.5).

106. The AT found that there was no detailed understanding in any of the authorities, of which legal persons are more at risk of being abused for ML. It is of particular note that whilst the Registry Agency is now appointed to act as the key gateway for registration of legal persons and arrangements and filing of BO information, its functions do not extend to considering risk that legal persons and arrangements present in Bulgaria; moreover, the authority was not represented in the NRA WG and so far, has had no role in the ML/TF risk assessment process in Bulgaria.

2.2.2. National policies to address identified ML/TF risks

107. During the period of the on-site evaluation, the Council of Ministers adopted an AML/CFT Action Plan. There was a two-year delay between the finalisation of the NRA report and the adoption of an Action Plan to address the ML/TF risks identified. The authorities outlined that this has been in part due to the impact of the COVID-19 pandemic in Bulgaria but that this has also been mitigated by the fact several actions, particularly major legislative changes identified as required by the NRA, have progressed in parallel to the development of the Action Plan.

108. The Action Plan is a comprehensive document on which the AT congratulate the authorities and particularly the FID-SANS who has driven the development and adoption of the Action Plan. Several actions are already underway, with some having made significant progress. The authorities outlined that despite the significant number of actions contained in the Action Plan, they intended for these to be finalised by the end of 2022 with an update of the NRA to follow thereafter.

109. The Action Plan outlines a number of the actions that are already underway as a result of the NRA across a range of areas.

110. However, whilst the Action Plan looks to determine an initial priority level and deadline, Bulgaria was unable to demonstrate that prioritisation and delivery is effective due to the recent time since adoption of the Action Plan. Equally, whilst the Action Plan lays out many significant projects for Bulgaria to complete in order to address ML/TF risks identified many are not national in nature but represent the work of a single agency.

111. The AT also consider that a major shortcoming for Bulgaria is the current lack of national policies to address major areas of risk identified in the NRA which are cross-agency in nature but represent a significant ML risk to Bulgaria. Examples of this include national policies to address ML risks related to corruption, the real estate and property sector and specifically the potential for abuse of the investment-related residence and citizenship (IRRC) programme and national policies which focus sufficiently on the ML risks related to corruption.

112. The Council of Ministers also adopted a National Strategy for Prevention and Counteraction to Corruption in Bulgaria (2021 – 2027)[23] which developed 7 main priorities and associate measures directed at strengthening the capacity and increasing the transparency in the work of anti-corruption bodies and units. However, it is unclear how the work on this strategy has specifically focussed on enhancing the activities of agencies preventing ML and not sufficient focus has been given to this area.

113. Equally, the significant risks identified from abuse of the investment-related residence and citizenship (IRRC) programme have yet to be adequately addressed by national AML/CFT policies. This is a particularly challenging area as it involves numerous agencies to co-ordinate an effective response (Bulgarian Investment Agency, Bulgarian Citizenship Directorate, Ministry of Foreign Affairs, Ministry of Economy, Ministry of the Interior, SANS). Generally, the AT found during the on-site that the Ministries had limited involvement in national policies and were not actively involved in co-ordination which was predominantly driven by operational agencies (such as the FID-SANS). Whilst some national changes have been achieved by amendments to the Bulgarian Citizenship Act which impact on the IRRC and the role of SANS to vet those acquiring citizenship, this has not been conducted under any clear national policy.

114. Although real estate related risks and vulnerabilities are among the highest in the NRA (incl. prevalent sale price manipulations), no national level policies have been introduced to address the significant ML/TF risks. It is of particular note that real estate agents are not subject to market entry measures (thus the size of the sector cannot be determined) and offsite supervision; and number of onsite examinations of the real estate agents by the FID-SANS is minimal. Whilst the Bulgarian system for the purchase and sale of real estate requires involvement of a notary, no steps are taken neither by notaries, nor real estate agents to establish whether the documented sale price is reasonable, and no steps are taken to establish or verify the original source of funds used for purchasing a property. There are no competent authorities appointed to verify whether the real estate price corresponds to the real market value. The 2019 NRA Action Plan includes some proposed measures which look to address some of the risks in the real estate sector by regulation.

115. Whilst both the very significant corruption risk and the risk of free-trade zones being abused for VAT fraud are noted in the NRA, these have again not yet been addressed by national policies to mitigate the potential ML risks identified. Whilst general policies around countering corruption have been produced by Bulgaria, these policies do not focus sufficiently on the financial links to corruption.

116. Overall, the AT considers that the lack of a National Strategy under which national AML/CFT policies could be developed is a significant shortcoming for Bulgaria. This is somewhat mitigated by the recent Action Plan which has been adopted, however, whilst some actions are underway it was not possible for the AT to confirm this was being implemented as a set of national policies in order to address AML/CFT risk. It is also unclear if the NRAM WG would function as an effective body for developing and approving national AML/CFT policies due to the fact the assessment team have concerns about its status, structure, and resources to fulfil its functions.

[23] Decision № 235 from 19.03.2021.

2.2.3. Exemptions, enhanced and simplified measures

117. Under the LMML, the exemptions, enhanced and simplified CDD measures are dependent on the established level of risk in the national risk assessments, the supranational risk assessment and the obliged entities own risk assessment.

118. Art 24 of the LMML and Art. 34 of the RILMML allows and exemption with regard to e-money however, in case of higher ML/TF risk identified, the exemption is not applicable. The exemption is limited in scope and is in line with the provisions of the 5th EU Anti-Money Laundering Directive (5th AMLD).

119. The regime in Bulgaria requires enhanced measures to be applied for PEPs, correspondent banking (with FIs outside EU/EEA area), new technologies (provided that the risks of new technologies are assessed as high in the NRA or business wide risk assessments carried out by the reporting entities), and higher-risk countries, obliged entities are also required to apply such measures in other high-risk situations as outlined in the LMML and RILMML. The situations under Bulgarian legislation that trigger applications of the enhanced measures are not derived on the basis of the national risks, but rather automatically transposed international requirements (i.e., FATF, EU AMLD). The LMML requires ML/TF risk assessments to be reflected in the internal rules of obliged entities and the risk profile of customers and the type of AML/CFT measures shall be determined based on the risk assessments.

120. Similarly, simplified CDD (SCDD) is only allowed based on established low risk of ML/TF and if the explicit and detailed conditions of the LMML and the RILMML are met, prior consent should be obtained from the FID-SANS which shall be seen as a positive risk mitigation measure. As noted under IO.4, the FID-SANS statistics show that in 2019 a total of 19 requests were made, 5 of which were refused (1 request was submitted by an arms dealer asking for the SCDD to be applied).

121. The BNB has outlined that banks reflect information from both SNRAs in 2017 and 2019, as well as information from the NRA in their internal AML/CFT risk assessments, which is then reflected in their AML/CFT procedures and relevant for the particular bank and use this information to justify the type of CDD for different risk scenarios.

122. Certain categories of OEs are not permitted to act as third parties according to R.17 (see analysis at R.17 for more information). The authorities demonstrated that this measure was justified on the basis of risks, i.e., the fact that non-core FIs and DNFBPs demonstrates lower level of compliance therefore should not be relied upon for the CDD purposes.

123. The AT identified a moderate deficiency in relation to the scope of the LMML which was the fact that the preventative measures and supervision does not extend to safekeeping of cash or other liquid assets (except where performed by a bank) as envisaged by the FATF standards. In Bulgaria, safe deposit boxes are offered not only by banks, but also by non-bank institutions, however, no controls or regulatory measures are in place. The Bulgarian authorities have noted that the use of safe deposit boxes is prevalent in Bulgaria and have particularly noted that unregulated safe deposit boxes feature in ML cases, therefore, the AT consider that this area can currently be considered an exception under the regime which cannot be justified. It is important to note that whilst the register of safe deposit boxes covers safe deposit facilities offered by banks, non-bank safety deposit boxes are not covered by the register leaving a sufficient deficiency.

124. In addition, entities providing payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank) and certain VASP activities, namely: persons providing exchange between one or more forms of virtual assets; transfer of virtual assets; participation and provision of financial services related to an issuer's offer and/or sale of a virtual asset are not subject to the AML/CFT and supervisory requirements (see c.1.6 and R.15, R.26).

125. Bulgaria has applied a cash limit under the Limitation of Cash Payments Act (LCPA) which prohibits certain entities from carrying out large cash transactions that exceed BGN 10 000 (€ 5 115) except in limited scenarios and the AT considers that this is effective in certain areas. DPMS have been exempted from AML/CFT requirements at national level, due to the application of the cash limit.

126. However, some activities do not fall under the scope of cash limitation, namely cash deposit and withdrawals from a person's own account held with a bank, payment institutions or e-money institutions, and currency exchange. While an exclusion of first party transactions with a bank, payment institution or e-money institution is justified, the AT does not consider that this has been justified for certain services that are not prohibited, which are normally services in the area of MVTS and currency exchange. The prevalence of large cash transactions in the banking and currency exchange sectors, often without plausible economic rationale (see CTRs table under IO.6) as well as cases of failing to report these transactions, leads the AT to question the overall effectiveness cash limitations introduced under LCPA as an AML/CFT control. R.1.

127. The AT therefore considers that at the current point in time in Bulgaria the assessment of risks is not properly used to justify all exemptions and support the application of enhanced and simplified measures. Risk assessments are only used to justify exemptions to some extent.

2.2.4. Objectives and activities of competent authorities

128. Bulgaria has demonstrated that the activities of the competent authorities were consistent with national AML/CFT policies and identified risks, to some extent, although this was a relatively new development. This was mainly due to the fact that the NRA process was relatively recently completed and whilst some actions more recently taken by authorities had been informed by the NRA work, the Action Plan to address the issues was only adopted during the period of the on-site evaluation. Outside of the NRA, Bulgaria was not able to demonstrate that objectives and activities were in line with risks and national policies. This was particularly due to the limited amount of ML/TF policies actioned at a national level.

129. The adoption of the Action Plan represents a political commitment to address the findings of the NRA but more generally the AT have concerns about the level of commitment and resources provided to AML/CFT efforts.

130. Considering the Risk Assessment and Ratings Matrix (part of the CoE Methodology), given the significant number of high/extreme impact and consequence level of risk events in Bulgaria, the AT considers that ML/TF policy work requires a significantly greater level of political priority in the country in order to deliver an effective AML/CFT regime. This issue is demonstrated by the period of 2 years that elapsed between the conclusion of the NRA exercise and the adoption of an Action Plan. Whilst the AT consider that the delay in adoption has been impacted by the COVID-19 pandemic, the AT were unable to confirm during on-site meetings that the area is given sufficient political priority.

131. That said, the Action Plan demonstrates a clear document based of the results of the NRA that Bulgaria is looking to address. The Bulgarian authorities have outlined that many of these actions have progressed in parallel with the development of the Action Plan and notably legislative actions have been completed.

132. Whilst FID-SANS are central to the NRA exercise and are the key co-ordinating body (therefore generally starting to align their activities to risk) during the course of the on-site, it was also demonstrated that some other authorities, particularly the BNB and FSC were able to demonstrate that they had taken some steps to align their activities to ML/TF risks.

133. The BNB has been involved in the creation of national AML/CFT strategies and policies and adjusts its policies accordingly in the period 2014-2019. The BNB was particularly involved in Working Groups concerning the transposition of various EU Directives. Equally, the BNB has produced two internal strategic plans for 2017-2020 and 2021-2023 which correspond to the national goals for improving effectiveness of AML/CFT measures in the banking sector. Conducting a sectoral banking level risk assessment was also as a result of EU Guidelines but co-ordinated at a national level by the BNB taking into account ML/TF risks.

134. FID-SANS has initiated activities in the format of expertise buildings (trainings) with particularly the BNB and FSC staff. Equally specialised AML/CFT supervisory units have been set up within the BNB and the FSC and there has been enhancement in international cooperation through participation in AML/CFT colleges by the FID-SANS, the BNB, the FSC. The BNB, the FSC and FID-SANS have also all updated their risk-based supervision methodologies in accordance with the NRA findings. Finally, the ability to implement administrative sanctions for non-compliance for the gambling sector has been introduced by the NaRA as the gambling supervisor; and FID-SANS now has access to the control servers of online gambling operators.

135. There has equally been some activity in the DNFBP sector with the creation of uniform internal rules for lawyers, notaries, auditors and accountants established with cooperation between FID-SANS and the relevant professional organisations and associations.

136. Some competent authorities who are critical to the AML/CFT regime in Bulgaria (such as FID-SANS, gambling regulator) are significantly exposed to prevalent governance related issues (triggered by the frequent change of the management) that might hinder the effectiveness of achieving strategical objectives, implementing operational action plans and overall, negatively impacting the domestic coordination and cooperation aimed at mitigating the risks. At the competent authorities' level, this might negatively impact the strategic objectives, continuity of operational plans, ability to retain expertise, etc. There is a direct example of negative consequences in this area demonstrated in relation to gambling supervisor (see IO3 for more information) resulting in inability by the competent authorities to supervise gambling sector.

137. Overall, the actions taken so far do not seem to cover all supervisory authorities concerned and it does not appear to the AT that the actions taken so far have been appropriately prioritised. The AT noted that very little action to increase resources of the supervisory authorities has occurred, which is of major concern (see IO3 for further information).

2.2.5. National coordination and cooperation

138. The AT consider that Bulgaria faces major issues concerning co-operation and co-ordination at both a strategic level in the development and implementation of policies concerning ML/TF and at an operational level concerning activities to combat ML and TF.

139. The AT were informed that the NRAM WG has been designated to continue the work of the NRA by the creation of the Action Plan and future co-ordination of ML/TF policies. The NRAM WG has driven the recently adopted Action Plan and demonstrates the only forum where national co-ordination occurs in Bulgaria either at a policy or operational level.

140. The NRAM WG is heavily reliant upon the FID-SANS to drive the work on development of national policies and actions and does not appear to have an appropriate structure, prominence or resources to develop the level of policies needed to address the ML/TF risks Bulgaria faces. A notable shortcoming is the lack of significant involvement of the major Ministries in driving the adoption of national policies in Bulgaria.

141. Considering the Risk Assessment and Ratings Matrix (part of the CoE Methodology) and given the significant number of high/extreme impact and consequence level of risk events in Bulgaria, the AT considers that national co-ordination of AML/CFT work requires a significantly greater level of political priority in the country and the adoption of adequate resources to ensure that national co-operation can occur effectively.

142. The AT do not currently consider that the NRAM WG has the appropriate structure, prominence, or resources to develop the level of policies needed to address the ML/TF risks Bulgaria faces. Whilst the authorities stated during the on-site that they believed the NRAM WG was effective and had suitable structure and resources in place to deliver its mandate – it was clear to the AT that the development of the Action Plan for the NRAM WG had been significantly challenging for Bulgaria and completing 53 high level actions by the end of 2022 will be equally challenging. Overall, Bulgaria was unable to demonstrate that the NRAM WG would achieve this aim or that resources would be sufficient to address the significant risks identified.

143. From the operational perspective, national cooperation occurs particularly between supervisors, and it was clear this did occur on *ad hoc* or supervisor to supervisor basis, however, this has not yet reached the stage of effective co-operation in a suitable forum at national level.

144. The lack of effective coordination and communication is considered by the AT to be significant in relation to supervisory matters. This resulted in confusion by the supervisory authorities met onsite in relation to their licensing and/or supervisory responsibilities. This led to the country struggling to demonstrate to the AT which authorities have an AML/CFT supervisory role – leading to some only being identified during the on-site visit. Also, as noted under IO3, the lack of effective coordination, combined with lack of aligned on supervisory policies result in duplication of the supervisory actions for some sectors (e.g., banks), whereas some other high-risk sectors are left with a very little supervisory attention (e.g., legal professionals, real estate sector, etc.).

145. In respect of co-ordination concerning law enforcement, it is noted (particularly in IO.7) that competent authorities are in most cases proceeding autonomously, without prosecutorial supervision and procedural deadlines and there is limited effective co-operation in this regard.

146. At an operational level, major concerns also remain about the overly formal approach to national cooperation, which can delay the timeliness of international cooperation (see IO.2).

147. The AT consider that the lack of suitable technology resources also impedes co-operation at a national level. There appears to be limited ability to share material, statistics or information nationally in a digital form which has notably impeded Bulgaria in conducting the NRA exercise. The AT consider this is an equal impediment to general co-operation at a national level and should look to be urgently addressed by Bulgaria.

148. Bulgaria demonstrated some positive early signs in relation to co-ordination relating to financing of proliferation of weapons of mass destruction (PF) and authorities with responsibility for proliferation have started to consider PF issues – however, currently there is limited co-ordination with key financial sector authorities (particularly ML/TF supervisors). Notably, co-operation at this stage predominantly focussed on proliferation issues (for example a working group drafting a law on restriction measures) without suitable consideration being given to the financing element of proliferation.

2.2.6. Private sector's awareness of risks

149. The executive summary, the risk events and the Risk Matrix on the NRA have been published at the official website of the SANS[24], however it was commented by met OEs at onsite that there was quite a considerable delay in publishing the results from the time that the NRA exercise and data collection commenced, which encompassed numerous years. The other method in which the private sector is aware of the NRA exercise is having been involved in data collection in different phases of the NRA process concerning the NRA conclusions, although engagement by the country with the private sector was more limited in this regard. In addition, FID-SANS provided 12 training sessions regarding the NRA in 2020 and the Bulgarian National Bank Specific Supervisory Directorate of the Banking Supervision Department (BNB-SSAD) also sent a circular letter to banks on the NRA.

150. As a result, the private sector has a general awareness of the NRA and its conclusions and the majority of OEs stated that they have integrated the findings of the NRA in their internal ML/TF risk assessments. However, the private sector met during the on-site felt that the information published on the NRA was not sufficient to develop their risk understanding beyond what already existed for their specific sector. The AT considers that this can be directly attributed to the fact that the private sector was involved in different phases of the NRA process to a relatively limited extent, published information on the NRA has been too minimal and there was limited outreach to the private sector.

151. There has been limited outreach to NPOs regarding their TF risks and to FIs and DNFBPs regarding NPO risks. This is particularly relevant in the context of TF and prevalent use of cash. This could be achieved by outreach activities to NPOs to detail risk factors and encouragement of transactions via formal financial channels.

Overall conclusions on IO.1

152. The AT is of the view that IO.1 is achieved to some extent, but major improvements are needed.

153. Bulgaria has made significant efforts in undertaking a comprehensive NRA process and producing a report based on reasonable sources of data and that has been subject to analysis across authorities and the private sector. The AT consider that the NRA Report 2019 and process demonstrates a reasonable general understanding across most authorities of the main ML risks that Bulgaria faces. The report contains a good initial analysis of the ML threats Bulgaria faces, however, the analysis of the vulnerabilities is not yet sufficiently developed meaning that the analysis of residual risk is limited. In some areas, there has been a reasonable analysis of the risks arising from various predicate offences (such as organised crime and tax crimes) while in other

[24] https://www.dans.bg/en/msip-091209-menu-en/results-from-national-risk-assessment

areas, understanding is hampered by lack of detailed consideration of the significant risks related to certain major predicate offences (such as corruption).

154. This relatively recent risk understanding is yet to translate into the development and delivery of national policies and procedures to address ML/TF. Whilst more recently some actions have been informed by the conclusions of the NRA, and the adoption of an Action Plan during the period of the onsite which looks to address the risks identified in the NRA exercise demonstrates progress, it is too early to demonstrate that this will translate into effective national policies to address the very significant number of ML/TF risks Bulgaria faces. The action plan is also significant with over 53 high level actions scheduled for delivery before the end of 2022. The AT do not currently consider that the NRAM WG has the appropriate structure, prominence or resources to develop the level of policies needed to address the ML/TF risks Bulgaria faces.

155. The lack of operational coordination and communication is considered by the AT to be significant in relation to supervisory matters and international co-operation. This led to the country struggling to demonstrate to the AT which authorities have a role in AML/CFT supervision and challenges with demonstrating international co-operation is effective.

156. Equally, the AT consider that Bulgaria faces major issues concerning co-operation and co-ordination at both a strategic level in the development and implementation of policies concerning ML/TF and at an operational level concerning activities to combat ML and TF which is further impeded by a lack of technology. Private sector awareness of national level risks is generally developed but the AT consider that the information published by Bulgaria on the NRA and outreach that has occurred so far is not sufficient to adequately develop awareness.

157. Not all activities that are covered by the FATF definitions for FI and VASP are subject to preventive and supervisory measures in Bulgaria. In addition, whilst DPMS are exempted from the AML/CFT requirements following the introduction of cash transaction threshold on the basis of risk, the exemption of other activities is not justified.

158. **Bulgaria is rated as having a moderate level of effectiveness for IO.1.**

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

a) Although a range of financial, administrative and law enforcement information is accessed by Bulgarian authorities, it is used in investigations and to develop evidence in relation to ML/TF and underlying predicate offences only to some extent. The timeliness and effectiveness of information analysis and exchange is limited by the lack of suitable IT systems on inter-agency and multi-agency level. The same issue is relevant to information exchange with the private sector.

b) The FID-SANS receives STRs, CTRs and information from state authorities. All STRs (in some cases also CTRs and other information) are reported to the FID-SANS on paper (in many cases accompanied by a CD) and delivered via postal services or couriers. In cases of urgency (postponement of transactions) STRs are reported to the FID-SANS via e-mail or phone call to the management followed by submission of a paper copy. Still, the current system in place cannot ensure prompt reporting in all cases and creates potential tipping off issues.

c) Bank account statements and other relevant information in many cases are analyzed in paper form, which significantly lowers the effectiveness, timeliness and quality of financial analysis carried out. Paper-based analysis also hampers the quality of financial intelligence actions throughout the procedural chain of analysis from the FID-SANS to judicial authorities.

d) The general quality of STRs appears to be good in the view of the authorities. However, the AT notes that a major part of STRs used for in-depth analysis is submitted by banks and MVTS (in many cases - defensive reporting). The general quality (and volume) of STRs submitted by other sectors, especially by DNFBPs needs improvement. There is very limited targeted outreach done to OEs to increase the quality and quantity of STRs. Based on the limited statistics available the AT concludes that the STR reporting is not commensurate with the countries` risks identified in the NRA.

e) The absence of clear procedures for the delay at the OEs of the STRs (transactions) sent to the FID-SANS for postponement has an effect on the allocation of resources and prioritization of the work of FID-SANS (especially in regard to STRs analyses being in line with the countries` risks) as they result in all postponement STRs handled with an utmost urgency. This can potentially limit the FID-SANS possibility to allocate resources to other STRs that would receive higher priority based on priority-risk-scoring-matrix (especially important in light of the fact that on the date of the onsite there was a significant volume of STR backlog).

f) As for the use of financial intelligence by most LEAs and prosecutors, limited and very formal feedback is provided to the FID-SANS. Generally, this does not allow the FID-SANS to adequately assess the quality of its analysis and disseminations and subsequently tailor its analysis to the needs of relevant authorities.

g) The FID-SANS conducts strategic analysis to some extent. The results of this analysis only to a very limited extent support the needs of other institutions. Topics of strategic analysis pieces are decided on an ad-hoc basis by the management of the FID-SANS. The FID-SANS has not had any training on strategic analysis. Strategic analysis is limited by the lack of their technical tools and resources.

h) The very limited availability of comprehensive statistics is a major issue for Bulgaria. The extent to which any statistics related to financial intelligence is kept is insufficient to allow the FID-SANS and other competent authorities to perform effective financial intelligence, set goals or analyse effectiveness thereof. The lack of comprehensive statistics limits the authorities' abilities to assess risks related to ML, associated predicate offences and TF.

i) There is no clear mechanism for dissemination of financial intelligence to competent authorities. The decision on recipient of dissemination is made on an ad-hoc basis and in some cases is unclear (in light of the fact that some authorities have duplicating responsibilities as analysed under IO.7). Many disseminations include recipients who do not perform criminal investigations and after adding some information from additional checks they forward the FID-SANS analysis to relevant competent authorities conducting criminal investigations. This significantly compromises the timeliness for potential investigations and possibility to timely identify and freeze or seize proceeds of crime.

j) The FID-SANS carries out very limited analysis on TF cases. Upon receipt of TF related STRs, with utmost urgency all available information to the FID-SANS is compiled and together with the STR information disseminated to the CTD-SANS. Although this allows the FID-SANS to disseminate information without any delay, it significantly limits the extent and quality of financial intelligence value added to the STR information. The quality of disseminations is also limited due to the low quality of TF related STRs.

k) The major lack of human and technical resources allocated to the FID-SANS hampers the quantity and quality of financial intelligence performed by the FID-SANS to support operational and strategic needs of its Bulgarian partners. The mainly paper-based information received by the FID-SANS is collected in a software-based and several excel-based "*databases*".

Immediate Outcome 7

a) The institutional framework for identifying and investigating ML offences is complicated and at certain points redundant, including authorities with overlapping or competing competencies and repetitive proceedings.

b) Many of the authorities involved (such as the AML Units within the MoI GDNP and the MoI GD-COC) are in lack of sufficient staff with adequate expertise and the necessary technical resources.

c) Pre-investigative operative proceedings are carried out without adequate supervision and there are no rules to prescribe examining the financial aspects of the proceeds-generating criminality, as a result of which no sufficient attention is paid to exploring any associated ML activities. Equally, the comprehensive understanding of the relevance of parallel financial investigations in the pre-trial stage could not be demonstrated either and there are no legal provisions or mandatory internal rules to require performing such exercises.

d) The prosecution appears to have overly high expectations as to the volume of operative facts and data required for initiating formal pre-trial proceedings. As a result, most of such referrals are rejected and the LEAs are instructed to gather more information, which results in delays and loss of efforts.

e) Extremely formalistic and bureaucratic features of the CPC pose unreasonable obstacles for the pre-trial authorities particularly as the strict and narrow deadlines and other procedural constraints are concerned.

f) Almost complete lack of meaningful and detailed statistics makes it impossible also for the Bulgarian authorities to have a clear picture of the composition and characteristics of the ML criminality in the country. The assessment was at many instances hindered by the lack of statistical figures or at least approximate estimations in this field.

g) Neither LEAs nor the prosecutorial authorities consider ML a priority and there are absolutely no mechanisms in place to prioritize any sorts of ML cases. All criminal cases are distributed randomly and dealt with equally.

h) The characteristics of ML offences investigated and prosecuted do not appear commensurate with the identified ML risks of the country, particularly as the composition of the respective predicate crimes is concerned. Most of the ML cases are related to fraud and have been generated by the reporting regime under the LMML, with almost no ML cases occurring in relation to high-scale corruption or organised criminality. There are no mechanisms or policies in place to achieve any significant changes in this field.

i) The number of ML investigations and convictions is generally low compared to the number of registered predicate offences in Bulgaria and the convictions achieved for such offences, at least partially because of the overly high evidentiary standards applied by the judiciary in ML cases. As a result of these standards, stand-alone (autonomous) ML offences are practically unknown in the Bulgarian criminal law.

j) In case of ML related to foreign proceeds, the expectations of the judiciary require that the details of the predicate crime be ascertained and demonstrated to a remarkably high extent which results in a mechanistic use of time-consuming MLAs instead of challenging the courts with more circumstantial evidence.

k) The criminal sanctions imposed for ML are generally very low, dominated by suspended imprisonment and moderate amounts of fines. This in most cases results from an agreement concluded between the prosecutor and the defence, which is not necessarily justifiable in every case.

l) The calculation of criminal sanctions imposable for multiple crimes, as prescribed by the CC often results in associated ML charges being practically unpunished if adjudicated together with a more serious offence.

Immediate Outcome 8

a) There is no legal or other mandatory requirement to pursue confiscation as a policy objective (e.g., by routinely launching parallel financial investigations or analyses), the use of which is thus subject to discretion both in the pre-investigative and pre-trial proceedings.

b) As a technical issue, confiscation from third parties is only provided for ML and TF offences while it is absent in any other relations including the provisional measures regime and the civil confiscation proceedings.

c) All provisional measures applied in the pre-trial proceedings are bound by strict and narrow, statutory deadlines which frustrates the securing of criminal proceeds in high-scale criminal cases. Provisional measures to secure property subject to confiscation are only taken in a very limited number of pre-trial proceedings.

d) Absence of any statistics (or other numeric data or, at least, approximate estimations) poses an insurmountable impediment to assessing the performance and effectiveness of the criminal (conviction-based) confiscation regime and the actual recovery of confiscated assets.

e) The technical side of the cross-border cash control regime is partially incomplete due to the lack of domestic legislation to provide for a legal framework for stopping and restraining cash/bearer negotiable instruments (BNIs) transported through the internal borders of the EU. The National Customs Authority has not demonstrated its capacity to detect and to restrain ML/TF related cash/BNIs.

f) There is no mechanism available for the active management of seized assets beyond storage and safekeeping measures by the CACIAF and for managing and disposing of property that has been confiscated under the CC, bearing a direct impact on effectiveness particularly if more complex types of assets have to be managed.

g) All authorities involved appear equally incapable to effectively secure, manage and recover virtual assets (VAs) despite the frequent occurrence of such assets in case practice.

Recommended Actions

Immediate Outcome 6

a) Human and IT resources of authorities performing financial intelligence activities should be substantially increased, especially FID-SANS (also relevant GDs of MoI; see IO7). This should include the development of an electronic systems for (i) the receipt and dissemination of STRs and other relevant data, (ii) document workflow of FID-

SANS, (iii) facilitate inter-agency information exchange, (iv) procure financial analysis software, as well as (v) basic technical needs of authorities (such as software to convert .pdf to. excel), etc., to enable more effective operational and strategic analysis and swift exchange of information.

b) The country should establish an appropriate mechanism and procedure for dissemination of financial intelligence information to competent authorities, with clear rules regarding the recipients of FID-SANS dissemination, based on competences of respective receiving authorities. The duplication of powers and responsibilities of certain authorities should be eliminated in order to make the process more efficient and effective.

c) LEAs and POs should increase the regularity and quality of feedback provided to the FID-SANS regarding its disseminations to ensure better support of their operational needs. The FID-SANS should keep comprehensive statistics and perform analysis on such feedback to ensure enhancement of quality of its disseminations.

d) The FID-SANS should significantly increase the quality and regularity of feedback and outreach provided to OEs regarding reporting higher quality STRs that would correspond to countries` risks.

e) Appropriate statistics keeping mechanisms and databases should be introduced within all institutions (especially FID-SANS) so that the analysis thereof could support the needs of competent authorities.

f) The country should ensure direct access to all relevant registers and databases is given to all LEAs, PO and specialized directorates of SANS and other competent authorities, responsibilities of which require such access.[25]

g) The FID-SANS should significantly enhance its strategic analysis function. Strategic analysis should be performed systematically in order to support the needs of FID-SANS` strategic goals, OEs, LEAs and other relevant authorities. Adequate training on strategic analysis should be provided to the relevant staff of FID-SANS.

h) The FID-SANS should take measures to further enhance its analysis and dissemination functions, including, introduce an adequate (more automated) prioritization system in order to clear the extensive backlog of STRs; agree on the needs of LEAs in regard to the substance of FID-SANS disseminations. FID-SANS should substantially increase the quality of its analysis in TF cases. Adequate training on financial analysis should be provided to all competent authorities.

i) Although not heavily weighted, the country should consider to set a clear procedure (process) at OEs in the transaction delay (postponement) mechanism.

[25] Access to (a) Bank accounts and safe deposit boxes register, (b) The Central credit register of bank loans, (c) Commercial register and Register of Non-Profit Legal Persons (CRRNPLP), (d) BULSTAT Register, (e) APIS Register information, (f) Real Estate register, (g) Tax authorities' databases, (h) Population register, (i) Registry of wanted persons, (j) Register of Criminal records, (k) Motor vehicles register, (l) Border control database, (m) Database for address registrations of foreign nationals, (n) VISA Register, (o) RegiX, (p) Social security and health insurance database should be granted to POs, directorates of SANS, all LEAs (where not already available).

Immediate Outcome 7

a) The authorities should revisit the institutional framework for identifying and investigating ML particularly in terms of redundant competencies. Clear division of competences should be achieved by issuance of the necessary secondary legislation but consideration should also be given to the establishment of a national/regional multi-agency targeting and coordination mechanism in relation to ML cases.

b) Concrete steps need to be taken for enhancing the specialization within LEAs by allocating more staff to the key MoI AML units and by providing adequate targeted training to the personnel. Technical resources of these LEAs should also be substantially increased.

c) A more adequate supervision of the pre-investigative proceedings by LEAs should be provided for, together with introducing and implementing rules as to when and how to examine the financial aspects of a proceeds-generating crime. In the pre-trial stage, the performance of parallel financial investigations needs to be stipulated in legislation or binding internal rules with adequate detailed guidance for the practitioners.

d) Internal rules or methodologies should be elaborated within the prosecution service to determine what level of operative facts and data should be accepted as sufficient for launching pre-trial proceedings so as to avoid the unnecessary duplication of efforts by LEAs.

e) The formalistic and bureaucratic characteristics of the CPC should be systematically revisited by the legislators so as to identify the obstacles caused by such features and to elaborate what legislative changes need to be carried out in this respect. As a priority, the regime of deadlines in Art. 234 CPC needs the most urgent reconsideration and modification.

f) Bulgarian authorities should make all efforts to maintain meaningful and detailed statistics on the composition and characteristics of ML cases investigated, prosecuted and tried in Bulgaria.

g) ML should be considered a priority by LEAs and prosecutorial bodies alike, by introducing adequate mechanisms to provide for the prioritization of ML cases.

h) Bulgaria should urgently elaborate and implement any necessary strategy or policy that is required so that LEAs and prosecutorial bodies pay due attention to a risk-based approach when identifying ML activities alongside the investigation of proceeds generating predicates and particularly cases of high-scale corruption or OC.

i) Internal methodologies or instructions should be issued, or trainings provided within the prosecutorial service so that the competent prosecutors maximize their efforts in challenging the judiciary with more ML cases, with a view to eroding the overly high evidentiary standards particularly by effective use of circumstantial evidence.

j) Similarly, internal guidance should be issued, or trainings provided to the competent prosecutors regarding the practice of concluding agreements with the defence so that this measure can be avoided in cases where the volume and quality of evidence available leaves no doubt about an imminent conviction.

k) Trainings or mentoring programs should be provided to judges, with a view to improving the performance of the judiciary, e.g. in the field of circumstantial evidencing or sentencing principles, without interfering with the judicial independence.

l) The current implementation of Art. 23 of the CC on the calculation of criminal sanctions for multiple crimes should be reconsidered and a more proportionate regime of sanctioning should be introduced with more extensive use of the existing mechanism in Art. 24 of the CC and, if necessary, adopting necessary changes to legislation.

Immediate Outcome 8

a) Wide-ranging and detailed statistics should be kept and maintained regarding the performance and volume of the provisional measures and confiscation regime as well as the assets that have been recovered.

b) Technical deficiencies relating to confiscation and seizure from third parties should urgently be remedied in the respective legislation (following the approach already applied in case of ML and TF offences).

c) The Bulgarian authorities should reconsider the deadline provided under Art. 234(8) CPC and enact appropriate legislative solutions for effectively mitigating the procedural constraints caused by such time limit.

d) Proceeds-oriented operative analysis should be made an integral part of pre-investigative proceedings performed by the LEAs. As for the pre-trial stage, a clear requirement to pursue parallel financial investigations needs to be issued together with clear and updated methodological guidance for the practitioners. Throughout the criminal procedure, the criminal asset recovery should be pursued as a policy objective.

e) Technical deficiencies under Recommendation 32 should urgently be addressed, particularly as regards the lack of Customs powers to stop or restrain cash/BNIs in order to ascertain whether evidence of ML/TF may be found. Measures should be taken to ensure that control of cross-border transport of cash/BNIs also takes into consideration identifying ML/TF suspicions and the Customs include in their focus the identified risks.

f) A comprehensive mechanism should be adopted for the active managing and/or disposing of property that is seized or confiscated, beyond the mere safekeeping measures.

g) The Bulgarian authorities should urgently establish the legal and technical conditions for securing, managing and recovering virtual currencies and extensive training should be provided to all authorities involved.

159. The relevant IOs considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are RR.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

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

3.2.1. Use of financial intelligence and other information

(a) Access to information

160. The competent authorities in the field of AML/CFT to some extent access a number of financial intelligence and other relevant information required to conduct their analysis and financial investigations, to identify and trace assets, develop operational analysis and investigate ML/TF and associated predicate offences. However, as described below some of the databases accessed by the competent authorities have deficiencies in the quantity and quality of information held.

161. The FID-SANS obtains information required to carry out financial intelligence by accessing a number of databases as provided in the Table 3.1 below. Also, FID-SANS receives STRs, CTRs, information on suspicion of ML/TF from state authorities, cross-border cash transportation reports submitted by the NCA. FID-SANS also receives information via domestic and international information exchange channels such as the Egmont Group.

Table 3.1: Access of available registers by Bulgarian competent authorities

Register name	Description of the register	Direct access
Bank accounts and safe deposit boxes register	Includes the holders and numbers (IBAN) of bank, payment and e-money accounts, persons authorised to use of the accounts, BOs of title holders of accounts, persons leasing safe-deposit boxes in banks and their attorneys, information on freezing orders on the accounts.	FID-SANS, specialised directorates of SANS, GDs of MoI, courts, PO, other investigative bodies, CACIAF
The Central credit register of bank loans	Includes information on all loans issued.	FID-SANS, specialised directorates of SANS, PO, other investigative bodies, CACIAF
Commercial register and Register of Non-Profit Legal Persons (CRRNPLP)	Central commercial and BO register (provides access to all documents uploaded on the files of each legal person and other legal entity, incl. financial statements).	FID-SANS, specialised directorates of SANS PO, GDs of MoI, Tax Administration, CACIAF
BULSTAT Register	Central commercial and BO register (provides access to all documents uploaded on the files of each legal person and other legal entity, incl. financial statements). Information on entities that are not listed in the CRRNPLP.	FID-SANS, specialised directorates of SANS Prosecutors, GDs of MoI, CACIAF
APIS Register information	Third-party held register with information CRRNPLP and BULSTAT Register with more functionalities for establishing commercial links between natural and legal	FID-SANS, specialised directorates of SANS

	persons, financial analysis function, social health insurance information.	PO (limited access), CACIAF
Real Estate register	Includes information on immovable property owned by natural and legal persons in Bulgaria.	FID-SANS, specialised directorates of SANS PO, GDs of MoI, CACIAF
Tax authorities' databases	Includes tax declarations for natural and legal persons, VAT declarations, incl. logs for purchases and sales, employment records for natural and legal persons.	FID-SANS, specialised directorates of SANS and CACIAF
Population register	Includes identification data on Bulgarian nationals and foreign nationals with residence permit in Bulgaria. The register also supports searches in Schengen Information System.	PO, GDs of MoI, FID-SANS, specialised directorates of SANS and CACIAF
Registry of wanted persons	information on wanted persons.	FID-SANS, specialised directorates of SANS, PO, GDs of MoI,
Register of Criminal records	Includes information on criminal registrations and convictions.	SANS, PO, GDs of MoI
Motor vehicles register	Includes information on vehicles owned by natural and legal persons.	FID-SANS, specialised directorates of SANS, PO, GDs of MoI and CACIAF
Border control database	Includes information on entries/exits through the borders for individuals and vehicles.	FID-SANS, specialised directorates of SANS PO, GDs of MoI,
Database for address registrations of foreign nationals	Includes relevant information submitted by hotels on reservations and stays.	FID-SANS, specialised directorates of SANS PO, GDs of MoI,
VISA Register	information on VISAs of foreigners.	FID-SANS, specialised directorates of SANS, PO, GDs of MoI
RegiX	infrastructure that enables the automated interconnections between multiple Bulgarian registries.	GDNP, CACIAF
Cross border cash declarations	Information on cross-border cash declarations.	Internal register of FID-SANS
Register of Persons Occupying Senior Political Positions	persons occupying senior political positions required to declare their property status annually before CACIAF as per the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act.	Publicly accessible information

Register "Edinstvo 2" (supported by the Notary Chamber)	The information includes issued Powers of Attorney. This is very relevant in the context of the use of straw persons in Bulgaria.	GD COC, FID-SANS, specialised directorates of SANS
Social security and health insurance database (employment)	current and past data on social security and health insurance records for natural and legal persons.	FID-SANS, specialised directorates of SANS, GDs of MoI, CACIAF

162. Different competent authorities have different levels and range of access to the listed databases. Although such approach is logical, in some instances the level of access is not sufficient. The FID-SANS has access to all of the necessary registers and databases, which can be accessed directly and in a timely manner. Specialized directorates of SANS and GDs of MoI have direct access to majority of the relevant registers and databases, while other LEAs, such as the those in charge of fighting tax crimes, have more limited access to the relevant information.

163. Apart from access to different databases, the LEAs also have access (upon request or spontaneously) to financial intelligence produced by the FID-SANS. The LEAs can obtain financial information from OEs directly or through the FID-SANS.

164. Regarding the access of information by LEAs directly from OEs, banking secrecy is an impediment that significantly limits timely access to banking information. Lifting banking secrecy requires an order approved by a judge, execution of which, together with administrative burden of sending the relevant documents in paper form, can take up to several months based on the practice of LEAs and some Prosecutors (see also analysis under IO.7). This is an issue for all competent authorities except for FID-SANS that can directly request the OEs for the information in case of a suspicion. The situation appears to be similar in regard to accessing tax information by certain authorities. For example, unit in the GDs of MoI conducting operational investigations on tax crimes does not have direct access to Tax Authority database, which is a major obstacle for effective work of the said authority.

165. Also, there are concerns about the accuracy of information held in some of these registers, for example, CRRNPLP and BULSTAT; especially in regard to BO information (for more detailed information, please refer to IO.5). This negatively affects the ability of competent authorities to access reliable information. It should, however, be noted that BO information can be accessed by FID-SANS and other competent authorities also through requests to OEs.

(b) Use of financial intelligence

166. Although, Bulgarian authorities have access to a range of financial, administrative and law enforcement information, it is used only to a limited extent in investigations and to develop evidence.

167. LEAs, prosecutors as well as specialized directorates of SANS obtain information from FID-SANS both as spontaneous dissemination and upon request. These disseminations include different types of information the FID-SANS has access to as well as the results of FID-SANS analysis. FID-SANS disseminations are of informative and analytical character. The information cannot be used as evidence in court and pre-trial proceedings. In most cases disseminations include information constituting an official, banking, trade or professional secret, as well as protected personal information and tax and social-security information obtained under the terms and according to the procedure established by the LMML.

168. The FID-SANS is generally considered to be an important source of financial intelligence for other specialized departments of SANS, and other competent authorities pursuing operation pre-investigations and prosecutions of ML, associated predicate offences and TF (please also refer to analysis under IO.7 and IO.9). LEAs and investigating prosecutors are requesting and FID-SANS is actively disseminating financial intelligence and other relevant information to Prosecution, LEAs and other competent authorities based on their requests. However, the overwhelming majority of such requests are from other specialized directorates of SANS. There is also no statistics available that could allow AT to conclude to what extent LEAs and prosecutors use the financial intelligence obtained from FID-SANS to develop evidence related to ML and associated predicate offences. The case examples provided by Bulgaria suggest that the financial intelligence is used to limited extent and mainly in investigating cases relating to fraud and tax evasion. As there are only two TF-related investigations conducted by the prosecutors it is difficult to conclude on the use of financial intelligence by the authorities for the purposes of TF investigations, also as FID-SANS never makes disseminations in relation to TF directly to prosecutors but to CTD-SANS instead. However, it appears that the use of FID-SANS information is very limited regarding TF investigations (for more detailed information, please refer to IO.9).

169. Some authorities have referred to the limited quality and the preliminary-analysis nature of FID-SANS disseminations. It should be noted that the timeliness and effectiveness of information exchange between relevant authorities and OEs spontaneously and upon request is limited by the lack of suitable IT systems on inter and multi-agency level (to access, exchange and analyse information on a timely manner). Moreover, there are major shortcomings identified regarding technical resources allocated to the FID-SANS. FID-SANS information is mainly collected in one internal software-based database. However, for in-depth operational analysis purposes several internal "databases' (excel based data sets) are used on daily basis. This to a large extent is limiting the quality and effectiveness of financial intelligence performed. Furthermore, there are no specific tools for the performance of adequate financial intelligence (e.g., such as lack of databases or other means to identify foreign PEPs was identified and would be very welcome by the authorities). The lack of electronic tools for data gathering and analysis generally hampers the quality of access and use of financial intelligence analysis of Bulgaria's competent authorities. There is generally a systematic lack of IT and human resources throughout all competent authorities (e.g., a basic program that changes bank account information from .pdf to. excel files is an extreme necessary due to the mainly paper-based-STR reporting system). Issues like access to scanners is also a limiting factor for some authorities to perform financial analysis.

170. Regarding technical resources of the FID-SANS - different tools are used for analysis, which include FID-SANS designed database, and some third-party IT tools, combining both information available and received. The information in majority of cases is received and analysed on paper. In many instances STRs are accompanied by CDs. Authorities informed the AT that currently, an EU funded Project under the ISF is being implemented aiming at the introduction of an IT software created especially for the use of FIUs. It is expected to improve the effectiveness of financial intelligence analysis and is very welcome.

171. There is also significant lack of human resources allocated to the competent authorities engaged in financial analysis (GDs of MoI, CCFCSCC-DEC of GD NP-MoI, GD COC-MoI) (see IO.7). The FID-SANS is in the process of increasing its capacity, including its human resources in the recent years, however, further improvement is still needed.

172. To conclude, a fundamental problem identified in regard to access and usage of financial intelligence by all authorities is the lack of IT systems and human resources. This significantly influences the quality of financial intelligence and its usage as there are major concerns by the AT that in many cases the "full picture" has not been identified due to the paper-based nature of data.

3.2.2. STRs received and requested by competent authorities

173. The FID-SANS receives information from OEs on cash transactions (CTRs). The Table 3.2 below shows the number of CTRs submitted by the OEs during the evaluation period. FID-SANS has indicated that this information is used for (1) the analysis of opened cases (operational analysis); (2) when relevant - for strategic analysis; (3) in the preparation of answers to information requests sent by LEAs and PO. However, it is not clear to the AT to what extent are these transaction reports analysed and used by the FIU in a systemic way. It should be noted that there is a back-log of CTRs.

Table 3.2: Number of CTRs submitted by obliged entities to the FIU

Year	2015	2016	2017	2018	2019	2020	31.07.2021
Banks	237 154	269 633	215 160	260 772	285 137	285 030	147 079
Currency exchange	1 458	3 927	3 821	6 882	6 882	8 820	3 750

174. OEs report STRs to the FID-SANS on paper (in many cases accompanied by CDs). In cases of urgency STRs are sent to FID-SANS via e-mail and management is notified of the STR via phone. However, also in these cases, the process is followed by submission of signed paper copy of an STR. The mentioned results in a process where all information, including, bank account statements are handled and analysed in paper form. Currently, this is a fundamental issue as it significantly lowers the effectiveness, timeliness and quality of financial analysis carried out by the FID-SANS. The paper-based analysis also hampers the quality of financial intelligence throughout the procedural chain of analysis (from the FID-SANS to judicial authorities). All STRs are delivered to the FIU via postal service providers (Bulgarian Post, DHL, etc.) or couriers of banks in sealed letters, which require signatures of recipients. This kind of procedure influences timeliness of submission of STRs (which, to some extent is mitigated by informal process of notifications to management of FID-SANS via phone) causes a potential risk of non-delivery of an STR and tipping off to the customer or potential customer. However, no such instances have been identified as explained by the FID-SANS.

175. As exhibited by the Table 3.3 below, the amount of STRs has been increasing throughout the period under review. However, the increase is predominantly due to the activity of money remittance service providers, although the quality of their STRs is very often low or the STRs are submitted in a defensive manner.

Table 3.3: Number of STRs submitted by obliged entities to the FIU – FIs

Year	2015		2016		2017		2018		2019		2020		2021 July	
STRs	All	TF	All	TF	All	TF	All	TF	All	TF	All	TF	All	TF
Banks	1762	15	2164	12	2157	12	2101	6	2280	9	2049	2	1259	2
Insurance:														

General insurance	5	0	0	0	2	1	5	1	0	0	0	0	1	0
Life insurance	0	0	1	0	1	0	0	0	3	0	2	0	6	0
Securities:														
Investment intermediaries	1	0	4	0	0	0	0	0	2	0	1	0	0	0
Management companies	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Currency exchange	5	0	12	0	4	0	3	0	2	0	3	0	1	0
Leasing companies	4	0	2	0	2	0	1	0	1	0	6	0	3	0
Postal operators (PMOs)	89	0	98	2	71	2	88	1	41	2	30	1	22	0
Money remittance	499	0	656	20	730	36	413	16	1765	12	2360	40	2320	8
Payment service providers (incl e-money)	11	0	9	0	54	0	129	0	394	0	457	0	456	0
Consumer credit	0	0	0	0	0	0	3	0	0	0	-	-	-	-
FIs registered by BNB	-	-	-	-	-	-	-	-	-	-	0	0	2	0
TOTAL - FIs	2376	15	2946	34	3021	51	2743	24	4488	23	4908	43	4070	10

Table 3.4: Number of STRs submitted by obliged entities to the FIU – DNFBPs

Year	**2015**		**2016**		**2017**		**2018**		**2019**		**2020**		**2021 July**	
STRs	**All**	**TF**	**All**	**TF**	**All**	**TF**	**All**	**TF**	**All**	**TF**	**All**	**TF**	**All**	**TF**
Gambling														
Gambling halls	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Casinos	4	0	6	0	5	0	8	0	4	0	0	0	0	0
Remote casinos	1	0	1	0	0	0	1	0	1	0	7	0	17	0
Real estate agents:	1	0	0	0	0	0	0	0	1	0	0	0	0	0
Dealers in precious	0	0	0	0	0	0	0	0	0	0	0	0	0	0

metals and stones[26]														
Lawyers	2	0	0	0	0	0	0	0	0	0	1	0	0	0
Notaries	5	3	2	0	1	0	3	0	1	0	7	0	6	0
Accountants	4	0	0	0	3	0	0	0	9	0	0	0	1	0
Auditors	0	0	0	0	0	0	0	0	3	0	0	0	0	0
CSPs[27]	0	0	0	0	1	0	0	0	0	0	0	0	0	0
TOTAL - DNFBPs	**17**	**3**	**9**	**0**	**10**	**0**	**12**	**0**	**19**	**0**	**15**	**0**	**24**	**0**

176. The overview of the STRs received shows that OEs do not face obstacles when filling in the STR Template. STRs are accompanied by all the relevant documents and information, but in some occasions additional information is requested from OEs with regard to the STR itself. As per explanations of the FID-SANS, the information requests are usually related to updating of bank statements, receiving information from another bank (not the reporting one) to receive up to date financial information.

177. As per the explanations provided by the relevant authorities, the general quality of STRs across the sectors (except for money remittances) appears to be good. However, the AT notes that a major part of STRs used for in-depth analysis are submitted by the banks. Authorities indicated that the second largest sectors` (i.e., Money remittance service providers) STRs are very often of low quality or defensive nature. Furthermore, authorities indicated that the general quality (and volume)[28] of STRs submitted by other sectors, specially DNFBPs, should be increased (see Table 3.4).[29] The FID-SANS has identified that major part of STRs do not contain a specific indication of the suspicion of predicate offence committed, although it in many cases is very clear from the text of the STR (mainly, tax-related crimes). The limited sample of corruption related (based on key-word search) STRs reviewed by the assessment team did not appear to be of good quality – STRs included very general description and not necessarily had specific indications to suspicion of ML or predicate offence or criminal proceeds being involved. Case examples provided in the Case Book confirm beyond doubt that the vast majority of ML cases reported, analysed and disseminated (see below), investigated, prosecuted and tried in Bulgaria are related to various forms of fraud (for more detail refer to IO.7).

Table 3.5: Break-down of STRs by predicate offences [30]

[26] Not obliged entities under LMML/LMFT due to limitations on cash transactions.
[27] Not obliged entities under LMML/LMFT as services usually carries out by legal professionals.
[28] E.g., Authorities indicated under-reporting from other sectors of OEs, which are not banks. They noted that in some cases banks report STRs where other OEs have not reported anything.
[29] E.g., as described under Immediate Outcome 4, currency exchange operators have filed insignificant number of STRs in the period under review. For example: in 2019 and 2020 respectively 2 and 3 STRs have been sent by all currency exchangers (almost 3 000 registered persons and some of them having larger networks which totals a large number of client service locations), while number of CTRs in 2019 and 2020 respectively were 7 205 and 8 820. In regard to DNFBPS - real estate agents, dealers in precious metals and stones and lawyers have altogether reported less than 10 STRs since 2015.
[30] As explained by the authorities, the information has been collected based on keywords included in the text of an STR. Through keyword search STRs were identified and reviewed to make sure

STRs with mentioned predicate offence[31]	2015	2016	2017	2018	2019	2020
Participation in an organized criminal group and racketeering	-	-	-	-	11	5
Terrorism, including terrorist financing	18	35	52	24	23	43
Trafficking in human beings and migrant smuggling	10	28	10	4	48	90
Sexual exploitation, including of children	1	1	3	-	16	7
Illicit trafficking in narcotic drugs and psychotropic substances	6	12	12	1	3	5
Illicit arms trafficking	1	8	9	1	3	1
Illicit trafficking in stolen and other goods	2	-	-	-	-	-
Corruption and bribery	1	5	1	2	3	5
Fraud	352	400	414	258	623	380
Counterfeiting currency	1	1	1	-	1	1
Environmental crime	-	-	-	-	1	1
Murder, grievous bodily injury	-	1	-	-	-	-
Kidnapping, illegal restraint and hostage-taking	-	-	-	-	-	-
Robbery or theft	-	1	-	-	-	-

that each identified STR concerns the specific predicate. Thus, the statistics does not contain double count.

[31] The figures in the table are results of manual search by keywords in the excel database.

Smuggling (including in relation to customs and excise duties and taxes)	4	8	5	-	-	-
Tax crimes (related to direct and indirect taxes)	24	314	28	1	20	9
Extortion	-	2	1	1	1	8
Forgery	1	3	13	6	2	8
Piracy	-	-	-	-	-	-
Insider trading and market manipulation	-	10	1	-	-	-

178. Some crimes that have been identified as high-risk in the NRA are not reported in STRs such as corruption, drug-trafficking, human-trafficking etc. (please refer to Table 3.5 on Break-down of STRs by predicate offences and Table 3.6 below). Moreover, there is very limited targeted outreach done to OEs to enhance the quality and quantity of such STRs. This is limited to dissemination of red-flag indicators and publishing of annual reports of the FID-SANS.

Table 3.6: STRs which include references to PEPs [32]

Year	Total number of PEPs related STRs	Foreign PEPs related STRs	Domestic PEPs related STRs
2015	37	6	31
2016	32	3	29
2017	20	0	20
2018	18	2	16
2019	17	0	17
2020	8	0	8
2021	14	0	14

179. In regard to analysis of whether or not STR reporting is in line with countries' risks, the AT was not able to fully identify relevant correlations due to the very limited breakdown of necessary statistics. Based on the limited statistics available (which the AT would examine in any other case; or, at least, approximate estimations as to what proportion the different predicate crimes represent in the ML criminality), as well as taking into account the cases provided in the Case Book, the AT concludes that the STR reporting is not commensurate with the countries` risks identified in the NRA. It should be commended, however, that upon receipt of an STR at the FID-SANS, the priority of an STR is determined based on a Priority Matrix, which corresponds to the

[32] This table contains data on STRs received on PEPs, ex-PEPs and also their relatives or close associates, i.e. – both persons under Art. 36(2) of the LMML and persons under Art. 36(5) of the LMML.

trends and risks identified in the NRA (the Priority Matrix has been updated after the adoption of the NRA in includes the relevant scenarios). Based on the priority it is decided whether or not the STR is sent to in-depth analysis. The case example below demonstrates the workflow of an analysis of PEP related STRs.

Box 3.1: Case example of FID-SANS analysis of PEP- related STR

In May 2021 FID-SANS received an STR containing information on a natural person identified by the OE as a PEP, on whose account in a suspicious operation were carried out amounting to over EUR 1.35 mln.

The review and analysis of the transaction documents performed by FID-SANS established that the person had received electronic securities in the amount of 22 mln. securities in connection with a contract concluded for consulting services with a foreign company. This PEP had acquired the right to sell the shares at a price that is many times higher than the market price. The FID-SANS established that in a short period of time (less than two months) more than 10 transfers were received, ordered from the investment intermediary opened in various commercial banks, amounting to over USD 1.6 mln. Each of the incoming transfers was in the range from USD 3 400 to USD 357 200.

In addition, FID-SANS performed checks in different databases (commercial register, registers of incoming notifications under the LMML /inquiries under the international information exchange / inquiries from law enforcement agencies /state institutions, register for import and export of currency in cash), to which FID-SANS has direct access. It was identified from publicly available sources that this person in fact was a Member of Parliament in the 40th, 41st, 42nd, 43rd, 44th, 45th and 46th National Assembly. A check was also carried out in the Register of Persons Occupying Senior Political Positions on CACIAF website, which found that the declarations of property and interests submitted by the person to the CACIAF did not contain declared equivalent forms of savings for the period from 2016 to 2020.

In connection with the suspicions that have arisen, as well as in view of the fact that the person held a senior state position, the information on the case was immediately disseminated to CACIAF, in order to carry out an inspection.

After a check in publicly available sources, it was established that based on materials provided in connection with an inspection carried out by CACIAF, the Prosecutor's Office of the Republic of Bulgaria has initiated an investigation in relation with a possible crime committed by a natural person – Member of Parliament. The pre-trial proceedings are for a crime under Art. 253 of the Penal Code.

180. Bulgaria's legislation allows OEs to submit STRs with indication of postponement (delay) of transaction or activity (pleases also refer to IO.3). The AT identified that the absence of clear procedures in the current postponement mechanism can hamper the FID-SANS` analysis of other STRs and has an impact on effectiveness. The lack of a legally defined period for the possible postponement (delay) for transactions or actions when reporting an STR with pending transactions gives the OEs discretion to decide for what period of time they are able or willing to delay the execution of a transaction or action. Although there are no statistics retained on such periods decided by OEs, the FID-SANS indicated that from their experience the shortest period is 2 hours and the longest - 7 days. All postponement STRs are handled with an utmost urgency, and not prioritised in accordance with the Priority matrix of the FID-SANS. The urgent action required to act before a lifting of the suspension by an OE might hamper the FID-SANS` ability to conduct

financial analysis in line with risk in the absence of sufficient time to assess the actual level of urgency and risk involved. Given the already limited resources of the FID-SANS, this might affect the allocation to higher priority STRs. The delay of transactions by the OEs precedes the postponement order issued by the FIU for 5 working days. Although authorities states that all OEs can delay transactions, it is not clear how the mechanism works especially, in regard to DNFBPs.

181. Examining the postponement/delay mechanism is also relevant for determining the quality of STRs and disseminations and the general effectiveness of reporting regime. In cases where there is a suspicion of ML or the funds are potential proceeds of a crime, the postponement order is issued by the FID-SANS. FID-SANS has the power to issue postponement of transaction or operation for a period of 5 business days. The postponement order can be issued upon the receipt of an STR, information on ML/TF received from state bodies, or information on ML/TF received in the course of international information exchange (including via FIU-FIU cooperation). Once a postponement order is issued, the FID-SANS has 3 business days (starting from the day succeeding the day of issuance) to inform the prosecutor of the suspension of an operation or transaction. The relevant prosecutor may subsequently approach the relevant court with a motion for the imposition of a freeze. The court must adjudicate on the motion within 24 hours from the receipt thereof. Where a freeze is not imposed within the given timeframe, relevant OE may carry out the respective operation or transaction. In case of suspicion of TF, the Minister of Interior or the SANS Chairperson or the officially expressly empowered (head of FID-SANS) may issue the aforementioned order. In addition to postponement mechanism, the FID-SANS has another special mechanism in place – FID-SANS has the power to request and OE to monitor transactions or operation carried out during business relationship to allow the FID-SANS to act and secure the potential proceeds of crime (ML/TF). Available statistics (where data is kept only for the period 2020 – 2021) suggest a large portion of transactions postponed by OEs were not followed by postponement orders of FID-SANS. However, most of the postponements of FID-SANS are followed by court freezing orders. The statistics on the extent to which FID-SANS postpones transactions not triggered directly by STRs is not kept.[33].

182. **Table 3.7:** Statistics on postponement order issues, transactions postponed

Year	Orders for postponement issued[34]	Transactions postponed	Total value of the postponed transactions in €	Number of postponement orders issued by FIU to suspend transactions/block account (which were followed by a court freezing orders)	Value of postponed transactions which were later frozen with the court orders
2015	11	20	20 467 455	10	20 356 775
2016	19	46	21 823 956	12	19 053 480

[33] For 2020 133 STRs were submitted before the execution of the transactions, and in period Jan-July 2021 the number of these STRs is 87.
[34] One order might refer to more than one transaction.

2017	6	19	1 923 468	6	1 923 468
2018	12	16	16 000 000	12	16 000 000
2019	41	85	27 185 561	36	24 687 589
2020	73	113	37 509 193	73	37 509 193
2021 July	17	116	2 511 443	17	2 511 443

183. The above-mentioned information on the powers of OEs to postpone transactions and the FID-SANS to impose monitoring and/or postponement should be taken into account in relation to the fact that at the time of the on-site visit there was a backlog of 3944 STRs that have not yet gone through preliminary analysis. There is also a 2-month backlog on CTRs to be entered into the CTR-database. The absence of clear procedures for OEs affects the allocation of FID-SANS resources in a way that is not in line with risk – potentially lower priority STRs with a delayed transaction are prioritized over STRs that would be of higher-priority in accordance with the FID-SANS` Priority matrix.

184. It should be noted that the FID-SANS informed the AT that the backlog of STRs is mostly low-quality defensive STRs and no urgent/high-profile cases are identified within the backlog. This information is based on a process in place, where an analyst checks the substance of these STRs even before the STR is entered into FID-SANS database and sent to preliminary-analysis and entered into the Priority matrix.

185. In accordance with Article 9 of the LMFT (parts one and three) any person, who knows that financial operations or transactions are intended for TF, shall be obliged to notify immediately the Minister of Interior and the Chairperson of the SANS. Additionally, whenever suspecting and/or knowing of TF, the persons referred to in Art. 4 of the LMML shall also be obliged to notify immediately the FID-SANS (via reporting an STR). Therefore, a triple-reporting-system is in place in cases where an OE has knowledge of TF. In practice based on the explanations of OEs the reporting is carried out only to the FID-SANS. OEs did not demonstrate knowledge on the necessity to report via additional channels.

186. Additionally, in regards to VAs, it should be noted that although several hundred (see Table 3.8 below) STRs related to virtual currencies had been submitted to the FID-SANS in the recent years and the relevant STRs are described by the FID-SANS to be generally of good quality – there is no possibility to perform any analyses due to lack of technical tools, there are no such tools also available for other Directorates of SANS or other competent authorities. The FID-SANS explained that these STRs concern bank transactions related to VCs rather than VC transactions as such (e.g., a person transfers funds from his bank account to bank account of popular foreign crypto exchange). There appear to be no STRs submitted by VASPs. With VASP sector in Bulgaria being relatively young, an increase in STRs is expected.

187. **Table 3.8:** Number of STRs related to virtual assets in the period 2017 – 2021 (July)

Year	2017	2018	2019	2020	2021 July
The number of VA-related STRs	48	92	91	99	124

3.2.3. Operational needs supported by FIU analysis and dissemination

188. FID-SANS is actively disseminating information related to ML and/or associated predicate offences to LEAs and prosecution as exhibited by Table 3.9 below, as well as information related to potential financing of terrorism.

Table 3.9: Disseminations of the FID-SANS based on the recipient

Year	MoI	Specialized Directorates of SANS	Prosecution	CACIAF[35]	Total
2015	179	524	17	-	720
2016	237	422	18	-	677
2017	281	468	11	-	760
2018	250	564	23	-	837
2019	90	274	30	15	409
2020	88	308	47	8	451
2021 July	39	159	15	8	221

189. As mentioned above, FID-SANS disseminations are of informative and analytical character. Law on credit institution and the CPC prescribe specific terms and procedure for the use of such information as evidence in court and pretrial proceedings.

190. Based on feedback received from specialised directorate of SANS dealing with financial security (FSD-SANS) it is established that only 36 FID-SANS disseminations were used in 2017 to trigger/support pre-trial-proceedings, that include pre-trial proceedings opened on the basis of information from FIU disseminations. In 2018 the number is 50, while in 2019 – 76.

191. According to feedback provided by the CTD-SANS for the period 2017-2019 the checks of disseminations of FID-SANS (both spontaneous and upon request) concluded that the general part of the information shall be used only for information-analytical purposes, while the checks

[35] The directorate referred to in Article 16 (2) of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act. This directorate is part of CACIAF from the beginning of 2018. Prior to that date, these functions were performed by a specialized directorate of SANS and, therefore, in previous years such information was disseminated to a specialized directorate of SANS with competence for corruption cases.

of 13 disseminations of FID-SANS concluded that the information shall be forwarded to Prosecutor's office or MoI.

192. According to feedback provided by GDCOC-MoI for the period 2017-2020, there were ongoing checks on 157 FID-SANS disseminations, checks of 113 FID-SANS disseminations resulted in decision to use the information only for information-analytical purposes, checks of 50 FID-SANS dissemination were sent to regional structures for COC, 4 were sent to GDNP or regional police structures, 88 – triggered/supported Prosecutors office's checks, and 20 disseminations triggered/supported pre-trial proceedings.

193. Based on feedback received from GDNP-MoI for the period 2017-2020, there were ongoing checks on 72 FID-SANS disseminations, 501 FID-SANS disseminations were sent to regional structures of MoI, 52 disseminations triggered/supported pre-trial proceedings.

194. FID-SANS also disseminates information to CACIAF, namely, the Anti-Corruption Directorate of the CACIAF, in cases where there is information on suspicious transactions carried out by the PEPs or high-level officials. There are no statistics available on follow-up of such disseminations. It should also be noted that CACIAF does not perform investigative functions and has no power to initiate criminal proceedings.

195. The above-described statistics on feedback received indicates that a significant volume of information disseminated form FID-SANS is only used for information-analytical purposes and does not result in initiation of criminal proceedings and further investigative actions.

196. It should be stressed that there is no clear mechanism for dissemination of financial intelligence information to competent authorities (e.g., based on the criminal offence identified) - the decision on recipient of dissemination is made on ad hoc basis by the person in charge of a sector or the management of FID-SANS (the mentioned is especially relevant, taking into account that in many cases there are two or more LEAs with overlapping powers and responsibilities). As described under IO.7, it is a particular feature of the Bulgarian AML/CFT regime that FID-SANS disseminations include recipients who do not perform criminal investigations (i.e., FSD-SANS, CACIAF) and only performing additional checks/analysis forward the FID-SANS analysis to relevant competent authorities tasked with investigating crime. These authorities perform financial intelligence actions (mirrors and adds to the work of FID-SANS) and to some extent activities of an operational nature to supplement the FID-SANS` analysis. Only after sufficient analytics is performed and data is gathered by these authorities a case is sent to the PO for decision on initiation of criminal investigation. These limited (mirroring) powers of respective authorities significantly prolongs the timeliness of potential investigations and possibility to timely identify and freeze or seize proceeds of crime.

197. As mentioned, the decisions on the dissemination and the specific recipient under Art. 75(1) of the LMML and Art. 9b(1) of the LMFT are made on a case-by-case basis by FID-SANS, taking into account the type and period of reported suspicious transactions, the scheme analysed, the existence or lack of indication for the predicate (as far as this might be important when deciding to which LEAs or prosecutors office the dissemination shall be made), the competences of the authorities listed in Art. 75(1) of the LMML and Art. 9b(1) of the LMFT, the existence of previously received request for the persons involved, etc. There have been no discussions between the FID-SANS and relevant LEAs regarding whether or not such ad hoc decisions are

appropriate and commensurate with the functions and needs of respective authorities. No MoUs have been concluded in this regard.[36]

198. The overwhelming majority of FID-SANS disseminations are disseminated to FSD-SANS, which to a large extent mirror and add to the analysis of FID-SANS by adding additional information from its own database. The FSD-SANS would normally not prepare their ML cases for being directly reported to the prosecutor - instead of which, most of their cases are forwarded to MoI bodies for gathering more information beforehand.

199. The process is different regarding STRs with postponement of transaction or activity. As described above, once a postponement order is issued by FID-SANS, the FID-SANS has 3 business days to gather information and disseminate it to the prosecuting magistracy of the suspension of an operation or transaction (the information is in parallel disseminated to LEA). The relevant prosecutor may subsequently approach the relevant court with a motion for the imposition of a garnishment or preventative attachment. The court must adjudicate on the motion within 24 hours from the receipt thereof. This procedure provides for a timely dissemination and effective freezing /seizure of potential illicit proceeds. In such cases, financial analysis is continued by FID-SANS and later disseminated to relevant prosecutor's office.

200. Regarding TF related STRs, the FID-SANS carries out limited analysis. Upon reception of a TF-related STRs, with the utmost urgency all available information to FID-SANS (STR information, information from registers) is compiled and together with STR information disseminated to CTD-SANS. Although this allows FID-SANS to disseminate information without any delay, as described further under IO.9 - it significantly limits the extent and quality of financial intelligence value added to the STR information (although, FID-SANS indicated that additional analysis is carried out after the case has been disseminated to CTD-SANS). This has also been indicated by the CTD-SANS via feedback to FID-SANS. It should also be noted that the quality of the FID-SANS products is also caused by the similarly low quality of TF-related STRs originating from the low understanding of TF-related risks by the reporting entities as described under IO.4 and IO.9.

201. In general, the law requires feedback to be provided to FID-SANS on every dissemination, however, in practice a very limited and formal feedback on the use of financial intelligence is provided by relevant authorities (the repealed LMML did not include a specific requirement for the provision of feedback, however, following the entering into force of this provision, this requirement is explicitly included in all FID-SANS disseminations, which is leading to an improvement of the regularity and content of the feedback the FID-SANS receives.). This approach does not enable the FID-SANS to adequately assess the quality of its analysis and disseminations and subsequently tailor its analysis to the operational needs of relevant authorities.

202. As for strategic analysis, the FID-SANS has neither a special unit to conduct strategic analysis nor specific analysts that would have had any relevant trainings. Although the FID-SANS conducts strategic analysis to some extent, the results of this analysis only to a very limited extent

[36] In regard to types of offences included in the disseminations of FID-SANS, FID-SANS provided an estimate information after the on-site visit that: around 10% of the dissemination contained indication of tax crimes, 15 % - fraud, incl. a couple of cases of counterfeiting and piracy of products, 15 % - corruption, OCG and human (incl. for sexual exploitation) and drug trafficking and migrant smuggling, illicit arms trafficking, and 3 % - TF. The rest of the disseminations do not contain indication of a specific predicate crime. This review covers period for 2020.

supports the needs of other institutions. Topics of strategic analysis pieces are decided on ad hoc basis by the management of the FID-SANS. An example of this type of analysis would be the NRA, the six-month reports and the annual reports of the FID-SANS, as well as ad hoc analysis on fraud cases, analysis on use of luxury goods and expensive vehicles for ML, and analysis on PEP-related operations. The FID-SANS has not had any training on strategic analysis and its capacity is limited by the lack of technical tools, human resources and most importantly the lack of statistics.

203. Major deficiency identified is the general lack of statistics. The extent to which any statistics related to financial intelligence activities is kept is insufficient to allow FID-SANS and other competent authorities to perform effective financial intelligence (especially – strategic analysis). The lack of statistics significantly limits the understanding of authorities of the risks related to ML, underlying predicate offences and TF. There is very limited possibility to measure effectiveness, the quality of STRs, effectiveness of FID-SANS` disseminations, cooperation with LEAs or other competent authorities, correspondence to risks identified in the NRA, set and measure their own performance etc.

204. Moreover, data and statistics gathering is a major manual work of FID-SANS, which also includes a large portion of manual paper-based work.[37] The mentioned has been an impediment to carry out day-to-day activities during the preparation of NRA. Although FID-SANS notified the AT about on-boarding of some new employees, still significant additional human resources would be necessary to adequately perform the core functions of FID-SANS. It should be noted that the current premises of FID-SANS do not appear to be suitable for the needs of FID-SANS. However, FID-SANS notified the AT on the fact that relocation to new – more suitable premises is planned to be fully finalized within 2022, once the new IT tool is technically implemented.

205. It should also be noted that there is general lack of trainings provided for staff that performs financial intelligence or financial analysis throughout competent authorities (e.g., Directorates of SANS, MoI GD's). At the same time, some representatives of competent authorities showed knowledge and professionalism in matters related to financial intelligence (FID-SANS` representatives showed a good level of knowledge), which does not exclude the need for additional specific trainings to be provided.

3.2.4. Cooperation and exchange of information/financial intelligence

206. Cooperation and communication among the authorities is carried out in a very formal manner, i.e., the overwhelming part of inter-agency cooperation and exchange of information is carried out through official written documents. There is very limited cooperation that would take other formal or informal forms.

207. Besides the spontaneous disseminations, Supervisory authorities, LEAs and Prosecution are requesting and FID-SANS is actively disseminating financial intelligence and other relevant information to Prosecution, LEAs and other competent authorities based on their requests. However, it should be noted that the overwhelming majority of such requests are from other specialized directorates of SANS. Additionally, the number of such requests has been slightly decreasing during the recent years as presented in the Table 3.10 below.

Table 3.10: Requests from competent authorities answered by the FID-SANS[38]

[37] It should be noted that a large part of statistics requested was provided during or after the on-site visit.
[38] This table contains information only for requests for information without prior dissemination on behalf of the FID-SANS

Year	MoI	Specialized Directorates of SANS	Prosecution	Supervisory Authorities	Other	Total number
2015	44	162	3	16	76	301
2016	18	241	2	5	36	302
2017	31	248	12	22	28	341
2018	16	256	8	6	13	299
2019	26	227	3	16	19	291
2020	14	229	2	13	2	260
2021 July	35	159	3	10	1	208

208. As noted above, a very limited and formal feedback on the use of financial intelligence is provided by relevant authorities. This affects very negatively the ability of FID-SANS to adequately assess the quality of its analysis and disseminations and subsequently tailor its analysis to the needs of relevant authorities.

209. The FID-SANS also engages in cooperation with supervisory authorities as shown in the Table 3.11 below. The FID-SANS cooperates with FSC and the BNB regarding licence applications. No information was provided on cooperation with other supervisory authorities in Bulgaria.

Table 3.11: Requests from competent supervisory authorities received by the FID-SANS

Year	BNB	FSC	Communications Regulation Commission	Total
2015	5	10	0	15
2016	1	4	0	5
2017	1	17	3	21
2018	1	5	2	8
2019	5	5	4	14
2020	3	2	7	12
2021 July	4	5	2	11

210. For detailed information regarding international cooperation of the FID-SANS with other relevant authorities, please refer to IO.2.

211. The AT identified some apparently minor issues regarding the autonomy of the FID-SANS. FID-SANS is a part of the SANS and there are some decisions and/or procedures that can be made or carried out only with the approval (signature) of the Chairperson of the SANS (e.g., on-boarding of new employees require the signature of the Chairperson of the SANS). As explained by the authorities, there have not been any cases where this would be identified as an obstacle. Additionally, the AT has concerns regarding the budget allocation to the FID-SANS.

212. During the on-site visit, the AT was informed that various security measures are implemented to protect information held within the FID-SANS premises, including information received from other FIUs, and to ensure that such information is being handled appropriately. The visit of the FID-SANS (and SANS) premises assured that security measures have been implemented with very high standards. The FID-SANS, however, informed the AT that it is moving to different premises.

Overall conclusions on IO.6

213. A range of financial, administrative and law enforcement information is accessed by the Bulgarian authorities. It is used in investigations and to develop evidence only to some extent. This is the case very much due to limited human and IT resources of the FID-SANS and the LEAs.

214. All STRs in some cases also CTRs and other information are reported to the FID-SANS on paper (in many cases accompanied by CDs) and delivered via postal services or couriers. The current system in place cannot ensure prompt reporting in all cases an creates potential tipping off issues. AT considers that the quality of STRs is better in the banking sector notes that a major part of STRs used for in-depth analysis are submitted by banks, however, it must be increased – both quality and quantity wise, - in all other sectors. Based on the limited statistics available the AT concludes that the STR reporting is not commensurate to countries` risks identified in the NRA.

215. Bank account statements and other relevant information in many cases is analysed in paper form, which significantly lowers the effectiveness, timeliness and quality of financial analysis carried out by the FID-SANS. Paper-based analysis also hampers the quality of financial intelligence throughout the procedural chain of analysis (from the FID-SANS to judicial authorities). There is no clear mechanism for dissemination of the FID-SANS information to competent authorities. This significantly compromises the timeliness for potential investigations and possibility to timely identify and freeze or seize proceeds of crime. The FID-SANS carries out very limited analysis on TF cases.

216. The FID-SANS conducts strategic analysis to some extent. The results of this analysis only to a very limited extent supports the needs of other institutions. The FID-SANS has not had any training on strategic analysis and is limited by the lack of their technical tools and resources.

217. The absence of clear procedures for the delay at the OEs of the STRs (transactions) sent to the FID-SANS for postponement has an effect on the allocation of resources and prioritization of the work of FID-SANS (especially in regard to STRs analyses being in line with the countries` risks) as they result in all postponement STRs handled with an utmost urgency.

218. The insufficient statistics in relation to financial intelligence does not allow the FID-SANS and other competent authorities to perform effective financial intelligence, set goals or analyse effectiveness thereof. The lack of comprehensive statistics limits the authorities' abilities to assess risks related to ML, associated predicate offences and TF.

219. **Bulgaria is rated as having a low level of effectiveness for IO.6.**

3.3. Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML identification and investigation

220. The legal framework for the criminalization of ML has not significantly changed since the previous round of evaluation. The ML offence includes almost all the material elements required by the international standards and the few technical deficiencies in this respect do not seem to have affected the case practice. Bulgaria has a complex institutional framework for investigating and prosecuting ML as well as for gathering criminal information relating to ML activities. Both in the operative and the criminal investigative stages of the proceedings, ML cases are dealt with by a range of various law enforcement and other authorities with partially overlapping or competing competencies.

221. A pre-trial investigation (i.e., a formal criminal investigation conducted pursuant to the CPC) is initiated and then directed by the competent supervising prosecutor. The procedure that in many cases precedes this investigative stage is the operative gathering of criminal information by LEAs, which information will then serve as a basis for the prosecutor to decide on launching a pre-trial investigation. In this operative phase, the competent authorities are in most cases proceeding autonomously, without prosecutorial supervision and procedural deadlines (except for certain cases mentioned below) while in the pre-trial phase, the objectives of the investigation and the necessary investigative measures are determined by the supervising prosecutor and merely executed by the investigators, who proceed under the command of the prosecutor.

222. As regards ML, the operative gathering of information on ML is in most cases triggered by the FID-SANS disseminations based on ML-related STRs. As discussed under IO.6 more in details, there is no clear mechanism in place at the FID-SANS to determine which LEA shall receive a given dissemination – instead, the recipient authority seems to be chosen on case-by-case (and to some extent random) basis. Among the possible recipients, one can find the two separate AML units within both central Police structures of the MoI, that is, the Sector of Crimes against Financial-Credit System and Cybercrime within the Economic Crime Department of the GDNP (GDNP AML Unit) and the Money Laundering Sector within the Corruption and Money Laundering Department of the GD-COC (GD-COC AML Unit).

223. Not only both MoI General Directorates (GDs) have separate units dedicated to the fight against ML but these central Police bodies show remarkable similarities in terms of their internal structure in general (for example, both GDs have one or more special units for drug crimes, corruption offences, cybercrime, or crimes against the cultural heritage). Both AML Units may receive FIU disseminations with not much differentiation except that ML cases committed in an organised manner or involving foreign proceeds would normally go to the GD-COC AML Unit. Apart from that, the ML-related competences of the two AML Units seem to overlap to a significant extent.

224. Lack of human resources have been emphasized by both AML Units. These comprise 10 staff members each, which in the view of the representatives of these structures, is not sufficient. As it was explained, the GDNP AML Unit deals with a number of other, equally serious economic crimes beside ML, while the work in the ML sphere is allotted to 2 operative officers only, which significantly limits their AML capacities. This might be one of the reasons why the majority of FIU disseminations received by this body would eventually be reassigned to regional (lower level) structures of the MoI (see under IO.6).

225. The GD-COC AML Unit is the only MoI sector (and the only LEA) exclusively specialized in countering ML of criminal proceeds, dealing with ML cases as a priority. However, they also consider themselves understaffed regarding their frequent involvement in assisting other GD-COC structures in identifying potential ML activities (particularly also because they have recently been demoted from a 20-staff department to a 10-staff subordinate unit). Considering this, the use of two separate AML Units for alternatively receiving the FID-SANS disseminations seems redundant and risks the waste of human resources. Also lack of technical resources has been identified in both AML Units.

226. It is a particular feature of the Bulgarian AML regime that he major recipient of FIU disseminations is the FSD-SANS which is not a LEA itself, rather a security agency with vast databases and analytical capacities. The FSD-SANS would normally not prepare their ML cases for being directly reported to the prosecutor - instead of which, most of their cases are forwarded

to MoI bodies for gathering more information beforehand. While all stakeholders agreed that the FSD-SANS input gives an important added value to the quality of ML cases being prepared, the subsequent involvement of multiple bodies in the process to build up a ML criminal investigation may duplicate the efforts and unnecessarily increase the time it takes for verifying a ML suspicion before finding it suitable for an investigation.

227. In the operative phase, ML activities can also be identified alongside the gathering of information on proceeds-generating crimes by the competent LEAs. In theory, there are no exclusive competences in this area and thus practically LEAs at all levels can collect information on associated ML activities. In lack of adequate statistics or at least approximate estimations, however, the authorities could not demonstrate in what proportion of the pre-investigative proceedings related to proceeds-generating crime the LEAs went on to follow the trail of the money and gathered specific information on the financial profile of the perpetrators and their associates that led to ML investigations. The AT learnt that such parallel financial examinations are rather unusual in the pre-investigative phase. The respective LEAs (and particularly the regional/territorial MoI structures) do not have sufficient time or even expertise to extend their activities beyond the predicate crime and thus cannot and will not pay due attention to the identification of proceeds of crime and to associated ML activities. There is no external (prosecutorial or other) supervision over the operative activities of the LEAs (unless the inspection is ordered by the prosecutor, who would then perform supervision) and neither are there internal rules or methodologies to prescribe exploring the financial aspects of a proceeds-generating crime. In cases where the prosecutor can order the performance of specific tasks before the pre-trial proceedings (see below) these are aimed at collecting further information on the predicate criminality rather than identifying any associated ML activities.

228. Regardless of the source of ML suspicion, the ultimate goal of all pre-investigative proceedings is to gather sufficient criminal information for convincing the competent (district or special) prosecutor to launch a formal pre-trial investigation which is then carried out by prosecutorial or Police (MoI) investigators under the guidance of the prosecutor. After completing their operative proceedings, LEAs thus present their findings in a report to the prosecutor who can either initiate a pre-trial procedure or send back the report by ordering further tasks to be carried out.

229. The law enforcement quite often struggles to meet the expectations of the prosecutors. Although it could not be determined with certainty whether this is because of the low quality of the LEA reports or the overly high standards of the prosecution, the AT are inclined to opt for the latter. All of the LEAs the AT met onsite opined that the volume of operative information required by prosecutors for a pre-trial ML investigation is very high and therefore LEA referrals are often rejected to gather more information. When exploring what proportion of such reports had been rejected, the AT was provided with prosecutorial statistics demonstrating a moderate frequency (4 to 8 cases per year from 2016 to 2021) while representatives of the GDNP and GD-COC explained that it had actually happened in almost every ML case.

230. When a report is sent back, the prosecutor determines which additional checks need to be carried out and sets a deadline to perform these tasks. All interlocutors met by the AT confirmed that at this stage, the main prosecutorial approach is to maximize the volume of criminal information that can be obtained in the pre-investigative phase so as to make a well-grounded decision on the initiation of the pre-trial investigation. On the other hand, the information gathered by LEAs in the operative phase cannot be considered and admitted as evidence in the criminal procedure (with a few notable exceptions such as data resulting from

SIMs). It means that every fact or data that has been established in the pre-investigative stage (pursuant to the Law on MoI or other sectoral legislation) must also be formally obtained again in the pre-trial proceedings in the form of evidence (in accordance with the CPC).

231. In addition, the prosecutors in Bulgaria require the maximum level of facts and data available before launching a pre-trial investigation so that all aspects of the case be checked beforehand. Specifically, in ML cases, this approach unavoidably results in delays both in initiating and eventually in carrying out a formal criminal investigation and prosecution considering the variety and complexity of facts and data to be obtained, including data protected by banking secrecy and, in case of foreign predicates, information from counterpart authorities abroad. The deadlines represent a further constraint: while operative proceedings initiated by the LEAs themselves are not bound by deadlines, those initiated by the prosecutor must be carried out in an extremely short (2+1 months) deadline after which the prosecutor must make a decision whether to pursue a pre-trial investigation or to terminate the case. All these factors taken together equally imply that a significant proportion of ML activities will eventually remain unidentified and/or neglected in the phase of operative information gathering by the LEAs and this handicap will unavoidably have repercussions in later stages of the proceedings.

232. A pre-trial investigation is initiated by a formal decision of the competent supervisory prosecutor who will then be the ultimate leader of the investigation (*dominus litis*) with an authority to determine and order the necessary investigative measures and to appoint an investigative body to execute these measures. Pursuant to the CPC rules, ML investigations are led by prosecutors of the competent District Prosecutor's Offices (DPO) or, in case of ML related to organised criminality, by the Specialized Prosecutor's Office (SPO). There are 28 DPOs in Bulgaria representing the second level in the territorial prosecutorial structure (the lowest level being the Regional Prosecutor's Offices).

233. The supervisory prosecutor is free to decide which authority shall investigate the case. It can be assigned to the same LEA that has performed the operative proceedings and made the initial report to the prosecutor, or to another LEA (any of the MoI GDs or their regional/territorial structures) in which cases the pre-trial proceedings will be executed by specific investigating police officers at the respective Police unit. As another option, however, the case can be assigned to the specific investigative bodies of the prosecutorial service. Each DPO has a separate Investigative Department attached, with an authority to investigate any of the cases within the competence of the respective DPO if so, decided by the supervisory prosecutor. The SPO also has its own Investigative Department with exclusive competence to investigate all criminal cases dealt with by the SPO. In addition, the prosecution service has a dedicated National Investigation Service (NIS) directly subordinated to the Prosecutor General for investigating cases of exceptional importance. A case can only be assigned to the NIS by the decision of the Prosecutor General upon the request of the respective DPO.

234. As it was confirmed on-site, approximately 95% of all pre-trial criminal investigations are carried out by investigating police officers while 5% is left for the investigating magistrates at prosecutorial investigative departments. As far as ML cases are concerned, however, the figures are significantly different. As it is illustrated by the Table 3.12 below, the proportion of district-level ML cases investigated by prosecutorial investigators has increased throughout the assessed period to the point that in the last few years, twice as many ML cases were dealt with by prosecutorial investigators than by Police bodies (the table does not contain data on investigations conducted by the SPO investigators and the NIS).

235. **Table 3.12** [39]

Pre-trial investigations regarding money laundering (partial data)									
		2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021 01-06**
Investigated by:	**investigating police officers**	101	108	135	73	89	47	65	31
	prosecutorial investigators	192	210	146	67	51	100	115	35

236. As a result, DPO prosecutors have a variety of different investigating bodies at their hand – which, however, has its pros and cons as well. Not all Police investigating bodies have the same level of expertise and experience in ML cases as the lack of professional personnel poses a problem even in the central structures (GDNP and GD-COC). Prosecutors the team met onsite generally expressed dissatisfaction with the quality of the investigative work performed by investigating police officers – and their desire to have more ML cases dealt with by prosecutorial investigators.

237. Similarly, to the pre-investigative phase, where the main challenge for LEAs is the high standards set by the prosecutors for initiating a pre-trial investigation, the main challenge in pre-trial proceedings is, as it was reported onsite, the high evidentiary standards set by the courts for proving the guilt of a defendant for ML. This demand has a direct impact on the scope and planning of a pretrial investigation, urging the prosecutor to obtain the utmost volume of evidence for all aspects of the ML offence before sending it to the court.

238. Case examples known to the AT perfectly illustrate that a wide range of various investigative measures are routinely deployed, and multiple databases consulted in most ML cases, which is commendable. It is another question however, whether all of these efforts were actually indispensable to sufficiently prove the case or only served to meet the overly high standards of the judiciary – as opposed to challenging the courts with cases more built on circumstantial evidence.

239. Parallel financial investigations alongside the investigation of proceeds-generating predicate crimes are not pursued routinely, as they are not formally required by any piece of legislation or mandatory instrument prescribing when and how to conduct such proceedings. There are some sources of non-binding guidance available to the practitioners such as the 2018 Methodology ("*Guidelines on establishing, tracing and securing abroad property acquired through criminal activity*) edited by experts from various bodies which is however already outdated.

240. Pre-trial authorities generally could not demonstrate a comprehensive understanding of the relevance of parallel financial investigations to identify criminal assets and associated ML

[39] This table includes all cases investigated during the given year, regardless of when the respective investigations were initiated (thus including pending cases from the previous years).

when investigating serious proceeds-generating crimes (some prosecutors the AT met appeared unfamiliar with the concept in general). As a result, such efforts are only taken sporadically in pre-trial proceedings. Even if associated ML activities are identified in course of the investigation of the predicate crime, corroborating the ML charges by evidence to the necessary extent is often time consuming (may require obtaining additional data and applying special expertise etc.) which would likely hinder the timely finalisation of the case with an indictment. In such cases, the prosecutor will focus on the predicate crime so that it can be thoroughly proven and brought before the court in a timely manner, while the associated ML is often separated and investigated in another procedure. The same happens if the predicate offence is investigated by a Regional Prosecutor's Office but the associated ML belongs to DPO competence. Such a forced separation might have a negative impact on the success of the ML case, particularly if it is not only separated but also assigned to a different Prosecutor's Office.

241. The situation is aggravated by some extremely formalistic features of the CPC which appear to pose some unreasonable obstacles for the pre-trial authorities. Pursuant to Art. 234 of the CPC an investigation must be completed within 2 months. Only in complex cases may the supervisory prosecutor extend this deadline by another 2 months, and if this is still not enough, a reasoned request must be submitted to the administrative head of the Prosecutor's Office for any further extension (maximum 2 months each). Every extension of the time limit also requires making a formal decision on any coercive measures being in force. This procedure is not only time-consuming and bureaucratic but failing to prolong this deadline will automatically render any investigative measures performed thereafter not to generate legal effect and evidence collected will not be admissible before the court. Another procedural constraint is Art. 234 (8) of the CPC which prescribes, that coercive measures taken in respect to the accused cannot last longer than 18 months in case of serious crimes or 8 months in all other cases, after which deadline they must be revoked (see under IO.8).

242. While these strict and narrow deadlines undoubtedly put an enormous burden on the pre-trial authorities and impede the effective and thorough investigation of more complex cases, the endlessly prolongable 2-month time limits would not necessarily prevent the occurrence of significant or even extreme delays in the pre-trial investigation, as it happened in one of the cases presented to the assessors:

243. **Case #35**

Box 3.3: Case example on ML investigation of proceeds of human trafficking

Between 2005 and 2006 3 individuals from Bulgaria trafficked women to France to work as prostitutes. They were prosecuted and convicted for this crime in France in March 2012.

The 3 individuals from Bulgaria received regular money transfers from France (90, 81, and 135 transfers respectively) resulting from the human trafficking they had committed.

The pre-trial investigation of the ML offence was initiated and performed in 2009 by the District Police Department of Shumen. However, 7 years passed without any significant result until Director of the National Investigative Service issued a decree on 18.02.2016 with which the pre-trial investigation was assigned to an investigator from the National Investigative Service. Finally, a thorough investigation was carried out, which itself took an additional 3 years and was completed by 24.04.2019. During these 3 years, a range of investigative actions were taken (by obtaining banking, tax, insurance, and company information to establish their property status; collecting evidence about the transfers they had received as well as about the senders of the transfers, their relations with the accused and the origin of the funds; identifying and hearing witnesses; obtaining evidence from abroad by means of EIOs etc.) as a result of which the 3 individuals were charged with ML offence committed to proceeds of human trafficking in the total amount of BGN 475 325 and were indicted before the court.

Finally, the case was filed in the district court with an indictment on 18.06.2019. Court proceedings ended in September 2019 when the court approved the agreement the prosecutor's office had concluded with the defendants.

244. Apart from some exceptional cases like this, the timeliness of the proceedings can mostly be provided for by the pre-trial authorities. Although no statistics were provided in this respect, the case examples the AT examined suggest that most investigations are completed in 1 to 3 years.

245. Beside the deadlines, the prosecutors generally complained on the extreme procedural formalism required by the CPC which, together with the lack of electronic communication channels between authorities, represents a significant delaying factor. As a typical example, the obtaining of banking data or document protected by bank secrecy was mentioned, the subsequent steps of which procedure (starting from the initial referral of the investigator to the prosecutor and ending with the production of the respective data or document by the financial institution) may take one or several months for the practitioners (at which time the initial information might already have become obsolete).

246. The special knowledge and experience required for handling ML cases is rather unevenly distributed within the prosecutorial service. While there are specific units for financial crimes at certain prosecutor's offices (such as the SPO) to concentrate such qualified staff, there are no such structures established in most of the DPOs. As a strict rule laid down by law and internal orders, the ML cases are distributed randomly among the prosecutors within a given prosecutorial structure (which means the aforementioned financial crimes unit in the SPO but the entire prosecutor's office in most of the DPOs). Further on, the ML cases enjoy absolutely no priority in the prosecutorial workload and are handled with the same attention as any other criminal case – hence there are generally no mechanisms within the prosecutorial service to prioritize ML or any sorts of criminal offences.

247. The Bulgarian authorities were unable to provide any statistical figures or at least approximate estimations as to what proportion of ML cases investigated and prosecuted had been resulting from the functioning of the suspicious transactions reporting regime and thus from FIU disseminations and/or reports directly from the financial institutions – and how many ML cases had been identified and pursued by LEAs alongside the investigation of predicate offences. The AT therefore had to resort to the collection of case examples provided by the authorities (see more in details below) and to information obtained during the onsite visit. It could be concluded beyond doubt that the majority of ML cases had been identified and initiated as a result of FIU disseminations and reports from banks. These are mainly related to various forms of fraud typically committed abroad and the laundering activities, which are investigated separately from the predicate, rarely go beyond the mere withdrawal or retransfer of illicit proceeds. The amounts involved are usually moderate.

248. The rest includes a number of cases where the predicate offence, typically trafficking in human beings, was committed abroad where it became subject of investigation and the laundering activities were likely identified alongside these foreign proceedings and then communicated to the Bulgarian authorities for further investigation. In this group, the ML is always self-laundering and consists of purchases of property items primarily in Bulgaria.

249. The last group is the one where associated ML activities were undoubtedly identified and pursued by the Bulgarian authorities in domestic investigations of proceeds generating crimes. The predicate crimes are typically fraud, tax crimes (VAT fraud) and unauthorized banking activity (usury) and the ML is always self-laundering in the form of purchase of property, investigated and in most cases prosecuted together with the predicate crime.

250. All these ML cases represent a limited seriousness both in terms of the complexity of the laundering activities and the volume of the proceeds involved. The Bulgarian authorities could not demonstrate their ability to successfully identify and investigate professional third-party ML with regard to proceeds derived from high-scale corruption or serious organised criminality, or ML committed by use of sophisticated international schemes and/or cryptocurrency. As for the latter, the AT notes that the awareness how to investigate and prosecute cases with virtual assets appears to be generally low in Bulgaria.

251. The limits of identification of potential ML activities can be illustrated by comparing the relatively moderate numbers of ML investigations and prosecutions to the numbers of reported proceeds-generating offences committed in Bulgaria:

252. **Table 3.13: Predicate offences**

Predicate offence	2015	2016	2017	2018	2019	2020
Participation in an organized criminal group and racketeering	160	88	82	103	106	89
Trafficking in human beings and migrant smuggling	541	408	211	134	125	179

Sexual exploitation, including of children	544	499	572	484	544	496
Illicit trafficking in narcotic drugs and psychotropic substances	3 724	4 445	4 713	5 211	5 147	4 560
Illicit arms trafficking	590	626	656	539	452	461
Corruption and bribery	390	678	668	620	490	478
Fraud	4 397	3 882	3 732	3 130	2 376	1 924
Counterfeiting currency	1 222	1 343	1 397	1 416	1 313	1 233
Counterfeiting and piracy of products	376	289	243	256	315	234
Environmental crime	40	44	51	31	58	98
Murder, grievous bodily injury	284	238	200	214	228	207
Kidnapping, illegal restraint and hostage-taking	75	70	102	64	72	81
Robbery or theft	52 296	44 735	42 976	38 646	33 576	27 547
Tax crimes (related to direct and indirect taxes)	41	319	372	451	470	367
Extortion	911	877	1 355	1 299	1 437	1 391
Forgery	3 348	3 408	3 538	2 998	3 131	2 720

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

253. As discussed under IO.1, the NRA highlights several major predicate offences as risk events thus representing the main threats for ML. Out of these, the risk related to the proceeds of corruption (particularly high-scale corruption including the abuse of EU funds) and the ML related to organised criminality (OC) were both considered to represent an extreme level of risk. In the context of OC-related ML, the NRA mentioned a range of proceeds-generating crimes

typically committed in an organised manner such as trafficking in human beings or in narcotics, which also represent threat on their own, rated as risk events with extreme and high level of risk, respectively. Other risk events linked to predicate offences are ML related to tax crimes (including VAT fraud) and smuggling (both rated having a high level of risk) as well as computer and social engineering fraud (representing medium level risk).

254. To assess the consistency of ML investigations and prosecutions with this risk profile, the AT would in any other case examine statistics broken down by the predicate offences with regard to the respective ML cases - or, at least, approximate estimations as to what proportion the different predicate crimes represent in the ML criminality. It was, however, impossible in Bulgaria where the AT were not provided with any sort of statistics or reliable estimation (with a notable exception mentioned below) to demonstrate what sorts of predicate crimes had generated the proceeds in the ML offences investigated, prosecuted and tried in the assessed period. Neither could the AT analyse whether and how the percentages of the respective predicate crimes change at different stages of proceedings (e.g. whether there are relatively more OC-related ML cases investigated but fewer of them prosecuted).

255. The lack of measurable figures relating to the characteristics of ML cases was, to some extent, mitigated by drawing conclusions from the analysis of the collection of case examples prepared by the Bulgarian authorities and incorporated in the Mutual Evaluation Questionnaire. This collection includes, among other, a remarkable number of ML cases investigated or prosecuted, the range of which was supplemented by additional cases mentioned during and provided after the onsite visit. Certainly, this collection (approximately 30 relevant cases) is the result of a selection made by the Bulgarian authorities and therefore it cannot be considered to represent the entirety of ML investigations, prosecutions, and convictions in the assessed period. Having said that, however, all these cases are valuable source of information and a basis for analysing the diversity and typical features of ML cases dealt with by the Bulgarian authorities.

256. Starting with the extreme risk events, no ML cases related to high-scale (or any sort of) corruption were provided or mentioned to the AT. Corruption of high-ranking officials has already been subject of several criminal proceedings (among the defendants a minister, a deputy minister and a judge were mentioned) but no associated ML activities have ever been subject of investigation or prosecution – even if in one of these cases, a part of the criminal proceeds was said to have been seized in cryptocurrency which appears to imply that some laundering activities had been carried out.

257. Laundering of proceeds from organised criminality can be found in the case examples but not with any remarkable regularity. The majority of such ML cases, that is 5 cases throughout the assessed period, related to human trafficking and showed remarkable similarities. The perpetrators were procurers and traffickers of prostitutes sent abroad for work, and the proceeds were the earnings the prostitutes regularly transferred to the perpetrators from abroad. All these ML cases thus related to quite simple forms of self-laundering – that is, receiving of direct proceeds of crime and using it for purchasing real estate or vehicles. The predicate crimes were subject of previous or parallel criminal proceedings in the respective EU member state (Italy, France, Germany etc.) and by the time of the conviction for the ML in Bulgaria, the perpetrators had in most cases already been convicted for the predicate offence. Neither of these cases can thus demonstrate the effective investigation of complex laundering schemes and that the domestic LEAs succeeded in identifying and pursuing OC-related ML activities.

258. Not a single ML case related to proceeds from high-scale and/or organised drug trafficking was reported by the authorities. Two low-scale drug-related cases could be found among the case examples, both related to laundering of own proceeds by purchasing other property items or simply by possessing the cash derived from drug trafficking. Both cases were investigated by regional/territorial MoI units, together with the predicate crime.

259. Another form of more or less OC-related predicate criminality represented in the case examples was the unauthorised banking activity (usury) which occurs three times in the collection of cases. Although at least one of these must have been committed in an organised manner, the laundering activities were quite simple again (purchase of vehicles or real estate) with moderate amounts of proceeds. Tax crimes related ML offences occur twice, without any specific particularities.

260. The case examples provided confirm beyond doubt that the vast majority of ML cases investigated, prosecuted and tried in Bulgaria are related to various forms of fraud. This was also apparent during the meetings onsite, where many of the practitioners the team met (from investigators to judges) appeared to have only or primarily dealt with fraud-related ML in their practice. Although fraud is also among the risk events (a less important one) listed in the NRA, the predominance of fraud-related ML cases is much more attributable to the relatively more effective functioning of the reporting regime as opposed to the identification of ML activities alongside the investigation of the predicate crime. Fraud-related ML is in most cases committed by strawmen in Bulgaria who withdraw or transfer funds, that is, proceeds of computer or social engineering fraud committed abroad, from bank accounts which is then reported by the respective obliged entities and eventually by the FIU.

261. The conclusions above can be corroborated by the only statistical information the Bulgarian authorities provided in the field of predicate criminality to ML. When preparing the NRA in 2016, the authorities manually searched the files of 89 ML-related criminal proceedings to determine what the respective predicate offences were and this is what they found:

262. **Table 3.14**

Number of criminal proceedings (Investigations, prosecutions and convictions summarized)	Predicate offence	Amounts € (when are available)
22	Computer fraud	3 103 971
2	Corruption and bribery	15 345
1	Counterfeiting currency	90 550
2	Forgery	820 811
24	Fraud	10 616 102
1	Illicit trafficking in narcotic drugs and psychotropic substances	2 996
1	Robbery or theft	2 156 000
1	Sexual exploitation, including sexual exploitation of children	309 248

3	Smuggling and other crimes in relation to customs and excise duties and taxes	N/A
12	Tax crimes	11 493 324
8	Trafficking in human beings and migrant smuggling	356 733
8	Unknown predicate	1 392 696
4	Other	13 635 336

263. In the year 2016, the situation was similar to today. Fraud-related ML cases were predominant, but human trafficking and tax crimes were equally represented with considerable numbers – while corruption offences and drug crimes appeared rather marginal with moderate amounts of proceeds.

264. Apart from specific predicate crimes, the NRA also highlights other risk factors such as the use of domestic and foreign legal entities for obscuring beneficial ownership, the laundering of funds through the construction and real estate sectors or the involvement of lawyers, accountants, and notaries in facilitating ML. These elements were almost absent from the case examples made known to the AT, with only sporadic exceptions such as the case below.

265. Case #52

Box 3.4: Case example with the use of domestic and foreign legal entities for obscuring beneficial ownership

The case was initiated on 18.02.2016 upon the report of a Bulgarian commercial bank "X" regarding a suspicious, yet unsuccessful attempt to withdraw cash from a bank account in the amount of € 20 000 at the branch of the said bank in Blagoevgrad. The pre–trial proceedings were then instituted in connection with materials received from GD-COC, which had previously been contacted by a different Bulgarian commercial bank "Y" with data on computer fraud and ML which materials were then forwarded to the local MOI unit investigating the case in Blagoevgrad.

The investigation established that the computer fraud, being the predicate crime in this case, was committed against two related Czech companies ("S Ltd" and "T Ltd") which both concluded trade contracts with a German construction machinery supplier "W Ltd" in February 2016. Under this contract, "S Ltd" and "T Ltd" both had to pay € 266 000 and € 75 600 respectively, to "W Ltd" as part of the agreed amount. As a result of a hacker attack on the parties' electronic correspondence, however, fictitious invoices for payment were sent to the Czech companies by unidentified perpetrators from a fake e-mail account, in which the seller's actual bank account was replaced by another one, opened by or on behalf of the perpetrators at the Blagoevgrad branch of Bank "Y" under the name of a Bulgarian company "O Ltd".

Deceived by the invoice thus received, both Czech companies transferred the aforementioned amounts to this bank account on 09.02.2016. Two days later, the total amount of € 320 800 was transferred from the account of "O Ltd" in Bank "Y" to another account held by a Seychelles company "E Ltd" in Bank "X" indicated as payment for computer services (the account from which the withdrawal was attempted on 18.02.2016.) From the latter account, the money was transferred to another person in a bank in South Africa.

To solve the crime, bank information was required for all movements on the accounts involved, including information on online banking with data on natural persons who could possibly have

done it and the IP addresses from which the access took place. Payment orders and invoices, on which the transfers of funds received as a result of fraud, were obtained. Information was required regarding the bank accounts of the representative of "E Ltd" and those of the related companies. A search was carried out at the home of the manager of the said offshore company and accounting documents were seized, as well as his personal computer and mobile phone. Forensic technical experts were applied who extracted information about relevant conversations and chats, as well as about other commercial companies related to the person. Information was requested from the company that assisted in the preparation of the documents for registration of the offshore company and it was established that the accused, who was its attorney in Bulgaria, had registered it. An EIO was issued to and executed by the Czech Republic for hearing the representatives of the injured Czech companies as victims.

The attorney was indicted as result of an agreement with the prosecution, which was approved by the court and the defendant was convicted on 27.10.2020.

266. Apart from this case, however, the characteristics of the ML offences investigated and prosecuted and particularly the composition of the respective predicate offences do not appear commensurate with the identified ML risks of the country.

3.3.3. Types of ML cases pursued

267. As it can be seen in Table 3.15 below, Bulgaria has achieved final conviction for ML offences in 8 to 12 cases per year from 2015 to 2020 in respect of 12 to 15 defendants altogether, which means that there was not more than one defendant in the majority of these cases. The annual figures for final convictions do not indicate any particular trends, oscillating around 10 cases/year throughout the assessed period. This is quite similar to the number of ML indictments which are roughly 20/year (with an exceptional low 12 in 2016) also without any noticeable tendencies, the main difference being the number of defendants involved which is significantly higher in the indictments (with an average of 1,8 individuals per case, indicating more than one defendant in the majority of the cases).

268. **Table 3.15** [40]

	ML Investigations by law enforcement carried out		**Prosecutions commenced**		**Convictions (first instance)**		**Convictions (final)**	
	Cases	**Persons**	**Cases**	**Persons**	**Cases**	**Persons**	**Cases**	**Persons**

[40] The figures in this table indicate the number of investigations initiated, prosecutions commenced, and convictions brought in the given year.

2015	**61**	**26**	**22**	**50**	**11**	**12**	**11**	**12**
2016	**59**	**8**	**12**	**21**	**12**	**19**	**8**	**12**
2017	**77**	**19**	**19**	**26**	**10**	**12**	**12**	**13**
2018	**73**	**5**	**19**	**34**	**10**	**17**	**8**	**15**
2019	**82**	**15**	**22**	**54**	**10**	**14**	**10**	**14**
2020	**85**	**12**	**19**	**23**	**11**	**16**	**10**	**14**
2021 01-03	**37**	**19**	**4**	**6**	**2**	**3**	**3**	**3**

269. The number of final convictions for ML is extremely low compared to the number of pre-trial ML investigations or indictments, and particularly disproportionate if compared to the overall number of convictions obtained for predicate offences as illustrated by the examples in the table below (the numbers represent the persons convicted.)

270. **Table 3.16**

	2015	**2016**	**2017**	**2018**	**2019**	**2020**	**2021 (01-06)**
Participation in an organized criminal group and racketeering	23	115	243	172	161	131	49
Trafficking in human beings and migrant smuggling	359	435	373	219	205	142	25
Sexual exploitation, including of children	35	34	38	47	33	26	6
Illicit trafficking in narcotic drugs and psychotropic substances	600	611	715	663	806	111	26
Illicit arms trafficking	299	310	346	267	270	258	64
Illicit trafficking in stolen and other goods	5311	4563	3519	3274	3130	3013	729
Corruption and bribery	92	129	124	156	126	101	18

Fraud	600	671	632	645	564	411	78
Murder, grievous bodily injury	84	80	80	83	76	75	10
Kidnapping, illegal restraint and hostage-taking	81	63	56	59	41	44	13
Robbery or theft	861	771	785	787	650	594	165
Smuggling	158	125	102	73	77	73	11
Tax crimes (related to direct and indirect taxes)	136	119	142	108	88	61	20
Piracy	145	167	97	120	89	125	34

271. The low number of convictions, as well as the lack of any tendencies in the numbers is not an indicator, rather a direct consequence of the equally moderate and stable annual figures for indictments and hence the output of the prosecution service in general. This phenomenon unavoidably raises some concerns about the quality of the prosecutorial work and the effectiveness of the prosecutors in developing and pursuing more ML cases particularly based on investigations into proceeds-generating predicate crimes. In any case, these statistics do not appear to indicate any efforts in this respect. Even though not all predicate offences may necessarily have had a ML-related aspect, such an enormous gap rather indicates that ML has not been a priority for the pre-trial authorities.

272. ML cases are tried at first instance by the respective District Courts or, in case of indictments submitted by the SPO, by the Specialized Court. As discussed below, the high evidentiary standards of the judiciary have had a direct impact on the success of the indictments submitted as a result of which a notable proportion of ML cases reportedly end up with acquittal despite the efforts of the prosecution to meet the standards of the court. This can also be seen in the statistics above which show that a notable proportion of the cases must have ended up with an acquittal, although the Bulgarian authorities did not provide any detailed statistics in this respect.

273. Although no prior conviction is required, the commission of the predicate offence must nevertheless be demonstrated with a remarkable level of certainty as regards the type of criminal offence as well as the time and place of its perpetration. As a result, it is not sufficient to prove that the laundered property is proceeds of some unidentifiable or unspecific criminal activity despite the fact that the ML offence follows an "*all crimes*" approach – and for the same reason, stand-alone or autonomous ML offences (i.e., those without any specifiable predicate offence) are entirely unknown in the Bulgarian law. If ML is not prosecuted together with the predicate offence, the latter must be demonstrated by concrete evidence – even in ML cases related to

foreign proceeds, where the prosecutors appear to seek MLA routinely and mechanistically for establishing the details of the predicate crime.

274. Among other critical factors, a direct connection between the predicate offence and the laundered property must always be proven by the prosecution and clear evidence must be brought for the mental element of the perpetrator, requiring the prosecution to prove that the defendant had knowledge of the criminal origin of the laundered proceeds. Furthermore, as demonstrated by Case 3.7 under Core issue 7.5 below, the Supreme Court's interpretation of third-person ML requires[41] that the prosecution establishes "*in an unequivocal and categorical way*" that the purpose of the act was not one's own enrichment, but to conceal the origin of the funds (or else the act can only be considered a receiving offence). Since this purposive element cannot be found in Art. 253 of the CC (where there is no purposive element at all) this judicial interpretation undoubtedly shows *praeter legem* characteristics.

275. All these high evidentiary standards, particularly as foreign predicates are concerned, represent a significant delaying factor, which does not seem to have been mitigated by use of circumstantial evidence.

276. In addition to that, ML indictments are reportedly turned down and routinely sent back to the prosecutor for correcting factual or legal errors as pointed out by the competent judge who also sets a deadline for this task. This power of the judiciary is applied with regularity, as a result of which cases can already be returned because of a typo in the indictment - but the AT were also made aware of more complex ML cases having been sent back because the judge had found the indictment being too complicated to comprehend. While the AT is not in the position to decide whether this practice has been caused by the low quality of prosecutorial indictments or the overly formalistic approach of the judiciary, the undoubtable procedural and evidentiary hurdles mentioned above pose an actual burden on the prosecutors discouraging them from challenging the courts with ML indictments based on less than the maximum level of proof e.g., by a more extended use of circumstantial evidence.

277. As for the different types of ML cases represented in the indictments and convictions, the AT were left, again, without any sort of statistical figures or approximate estimations and therefore the country failed to accurately demonstrate that all sorts of ML can be subject to prosecution and conviction in the legal practice of Bulgaria. The AT had to resort, again, to the collection of case examples mentioned above, which appears to confirm with due certainty that Bulgaria has actually obtained ML convictions for both foreign and domestic predicate offences and also for cases of 3rd-party and self-laundering alike. No further conclusions could however be drawn as to the proportion of these features within the entirety of the ML indictments or convictions or any trends in this respect.

278. The analysis of the case examples has also demonstrated that most of the 3rd-party ML offences were prosecuted separately from the predicate, while most cases of self-laundering were typically prosecuted together with the underlying predicate crime except for those related to foreign predicates. In cases where foreign proceeds were laundered (3rd-party or own proceeds ML alike) the case examples demonstrated the significant efforts the prosecution had to put into bringing evidence for the predicate crime. While in certain cases it could be corroborated by a prior conviction (as it was with the ML cases related to organised human trafficking in EU

[41] Decision № 499 of 12.03.2015, case № 1777/2015 and Decision № 200 of 04.01.2017, case № 744/2016.

member states) in many instances MLAs had to be sent out before bringing the case to the court so as to ascertain the details of the foreign predicate crime. In a number of cases, this approach went to extremes to meet the expectations of the judiciary, just like in the following example.

279. Case #59

Box 3.5: Case demonstrating significant efforts by the prosecution to collect evidence on predicate crime

Initially, a sum of money in the amount of €250 000 was received on the bank account of a Bulgarian commercial company, with which bank orders were made, by a proxy of the trader. Subsequently, other orders were received and executed with different amounts of money.

The predicate crime was identified as fraud or misappropriation of property committed on the territory of the Republic of Italy by employees of an Italian legal entity. The predicate offence was subject of an investigation in the country where it was committed, where there is evidence that an effective judicial act has been issued by the Italian court.

In the Bulgarian investigation, bank information was obtained about the ownership of the Bulgarian bank account and the movement of cash on the latter. Graphic expertise of the signatures in the bank documents and forensic accounting expertise on the movement of funds in the bank account have been prepared.

In addition to that, an EIO has been issued to the Italian authorities for hearing of witnesses and requesting further evidence of the predicate offence. Furthermore, an additional EIO is being prepared for obtaining the court act for the predicate offence. The investigation is ongoing.

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

280. Analysis of the cases provided in the collection of case examples mentioned above shows that the main sanctions applied for ML offences are custodial sentences. The ML offence in Art. 253 CC is threatened with imprisonment that can be imposed within the following limits:

- 1 to 6 years (basic forms of ML in para 1 and 2)
- 1 to 8 years (if committed in an organised manner, repeatedly, etc. in para 3)
- 3 to 12 years (related to proceeds of a serious intentional crime in para 4)
- 5 to 15 years (extremely large amount or extremely grave case in para 5).

281. The range of punishment above is quite dissuasive - but it does not appear to have much effect on the judicial practice in sentencing for ML.

282. As it is illustrated by the Table 3.17 below, most of the criminal sanctions imposed for ML are indeed imprisonment which are, however, suspended for a probation period. According to Art. 66(1) CC the maximum term of imprisonment that can be suspended is 3 years, which can be suspended for a probation period of 3 to 5 years. It means the 3 years suspended for 5 years is the maximum term of a suspended sentence – and this is exactly the sanction that has been met out most often in ML cases in the assessed period.

283. **Table 3.17:** Criminal sanctions imposed for ML

Year	Non-custodial sentences			Custodial sentences		
	Fines (€)	Other than fines	Total number	Imposed prison sentence (persons)	Suspended prison sentence (persons)	Total number (persons)
2015	4 persons Total: € 25 000	1	5	4	21	25
2016	7 persons Total: € 118 000	-	7	7	6	13
2017	6 persons Total: € 21 000	-	6	3	16	19
2018	8 persons Total: € 60 000		8	7	12	19
2019	6 persons Total: € 38 000	-	6	5	12	17
2020	15 persons Total: €128 622	1	16	5	15	20
2021 01 - 06	2 persons Total: €10 000	0	2	1	1	2

284. In most of the case examples concluded with a conviction, the typical sentence was 3 years of imprisonment suspended for 5 years, or even less. This primarily refers to a large group of almost identical ML cases (consisting of transfer or withdrawal of money from bank accounts, which constitutes proceeds of fraud committed abroad) subsumable under one of the basic forms of ML punishable by imprisonment from 1 to 6 years. In addition to these, however, the AT noted further ML cases in which the characteristics of the ML offence would normally not call for such a lenient sentence. The latter group included cases of ML committed in relation to organised forms of human trafficking, or to usury committed in an organised manner, most of which cases were prosecuted by the SPO. As these forms of ML appear to fall under the aggravated cases in para (3) or (4) punishable by more severe sentences, a suspended imprisonment appears less justifiable. As a consequence, the assessors are concerned that this high rate of suspended sentences impacts negatively on the effectiveness of sanctions.

285. According to the prosecutors the team met onsite, the main factors that apparently contribute to the predominance of suspended imprisonments are the moderate seriousness of the respective ML cases and the generally mild sentencing principles. It needs to note, however, that no particular dissatisfaction with this sentencing was expressed by the prosecutors and the AT was not made aware of any formal or informal guidance or systematic policy by the prosecutors to appeal lenient sentences for ML handed out by the courts.

286. Subsequently, the thorough analysis of the case examples demonstrated another factor: the agreement between the prosecution and the defendant. Such agreements to dispose of the case (so as to avoid a lengthy trial) are governed by Chapter 29 CPC and usually result in less severe punishments than what would normally be imposed. An agreement was mentioned in almost every case concluded with a suspended sentence and therefore the generally mild sentences must, to some extent, be attributable also to the prosecutorial policies in this field. While this approach will undoubtedly ease the procedural burden on the prosecutor and the judge in the trial stage, no perpetrators will eventually be punished by a dissuasive sentence which may have negative consequences particularly in the more serious cases of ML mentioned above.

287. In the few cases apparently not ended with an agreement, the terms of imprisonment imposed for ML ranged between 2 to 6 years. These punishments can be considered sufficiently dissuasive and proportionate, but again, these are only the notable exceptions.

288. Another factor that seriously limits the dissuasiveness and proportionality of the sanctions is the way the Bulgarian criminal law handles cases with multiple crimes. Art. 23 CC provides that if by one act several crimes have been committed, or if a person has committed several separate crimes before the issue of sentence that has entered into force for any of them, the court shall, after determining punishments for each crime separately, impose the most severe thereof. (This rule applies to punishments of the same kind, that is, to the most severe imprisonment and the most severe fine.) While in theory this means that no crime will remain unpunished (as punishments would technically be determined for each offence) in practice the less severe punishments will entirely be consumed by the most serious one. As it was illustrated by more than one case examples, this usually means that whenever ML is prosecuted and tried together with a more serious predicate offence, only the punishment determined for the predicate crime will have to be served by the defendant and whatever would have been imposed for the associated ML will not be considered.

289. It needs to note that in such cases, Art. 24 of the CC allows the court to increase the determined total most severe punishment by at most one half in order to give consideration to the weight of the other, less serious crimes (the punishment thus increased may not exceed neither the sum total of the separate punishments, nor the maximum extent provided for the respective kind of punishment). In the selected case examples, however, the AT could not find any ML case where this rule was applied by the court.

290. Case #50

Box 3.6: Case example on imposed sanctions[42]

Upon completion of the investigation, 3 defendants were brought to court. On 13.02.2018 the District Court of Pernik convicted Defendant #1: (i) for performing unauthorized banking activities to imprisonment for a term of 5 years and 4 months and a fine in the amount of BGN 6 000 (€ 3 067); (ii) for ML to imprisonment for a term of 4 years and a fine in the amount of BGN 10 000 (€ 5 113; (iii) and for tax fraud to imprisonment for a period of 4 years. Pursuant to Art. 23, paragraph 1 of the CC the defendant was finally sentenced to one general, most severe sentence of imprisonment for a term of 5 years and 4 months, and a fine in the amount of BGN 10 000 (€5 000).

With the same sentence, Defendant #2 was convicted of ML and sentenced to imprisonment for a term of 3 years and a fine in the amount of BGN 5 000 (€2 556) and, for tax fraud, to imprisonment for a term of 2 years and a fine of BGN 1 000 (€511). Pursuant to Art. 3, paragraph 1 of the CC he was sentenced to one general sentence of imprisonment for a period of 3 years, the serving of which was postponed for a period of 4 years. A fine in the amount of BGN 5 000 (€2 500) was added to this punishment.

291. This is an additional procedural obstacle the prosecutors must bear in mind when preparing a ML case for indictment – whether to prosecute both the predicate crime and the ML together so as to better meet the high evidentiary standards of the judiciary, or to separate the case into two so that the perpetrator be effectively punished also for the ML offence.

292. Fines are routinely imposed together with (suspended or executable) imprisonments within the limits defined by law. These limits are however disproportionately low (see the analysis under c.3.9) and thus the fines cannot be considered dissuasive. Art. 23 of the CC mentioned above also refers to fines (only the highest of the possible fines will finally be imposed).

3.3.5. Use of alternative measures

293. As it was explained by the authorities, if pre-trial proceedings for a ML offence do not bring sufficient evidence for ML but for another crime, such as the material concealment in Art. 215 of the CC (a classic receiving offence with lower evidentiary standards and milder sanctions, being only applicable to movable items of another, derived from crime) charges are routinely brought for this crime. A typical case example can be read below.

Box 3.7: Conviction on predicate offence only despite of having evidence also on ML

Defendant M. stole cash in various currencies totalling BGN 8 267 from an apartment, then visited defendant N. and told him about the theft he had committed. M. left some of the stolen money in amount of BGN 5 876 (€3 004) at N. asking him to keep it with him. On the following day, they went together to a car dealership and bought a car in the name of N. with BGN 2 500 (€1 278) derived from the theft. On the same day, they went to different stores, where N. bought various electronic products with the stolen money in the amount of approx. BGN 950 (€485) while he spent BGN 480 (€245) to prepay a three-month rent for his accommodation. One day

[42] The description of the ML offence is not relevant here and thus not provided.

thereafter N. paid the rest of the money left to him, that is BGN 2 390 (€1 222) to his bank account, from which in the following days he withdrew and made payments totalling BGN 785 (€401) including twice giving money to his accomplice M. at his request.

The Ruse District Court found them both guilty – M. for aggravated theft and N. for ML. As for the latter, N. was convicted for receiving, holding, using and transforming property, which he knew at the time of its receipt had been acquired by M. through a serious intentional crime, and performed transactions and financial operations with this property thereby concealing its origin and the actual rights over that. N. was sentenced to 4 years of imprisonment and a fine of BGN 20 000 (€10 225).

While the competent Court of Appeal confirmed the verdict, it was then overturned, in respect of N., by the Supreme Court of Cassation, which returned the case for reconsideration because the subjective side of the ML offence (the motivation of the crime) had not sufficiently been proven. The Court of Appeal re-adjudicated the case and in its new verdict (which was later upheld by the Supreme Court) found that N. had committed the offence of material concealment (Art. 215 of the CC) and not the ML offence (Art. 253 of the CC).

As it was expressed by the Supreme Court of Cassation, the actions of N. may constitute, from an objective point of view, the elements of the crimes under both Art. 253 and Art. 215 of the CC "*as the essential difference between the two compositions is in the constituent special purpose*". The transactions N. carried out (acquiring various property items in his own name and depositing part of the funds in his own bank account) objectively corresponds to the features of the ML offence "but for this qualification it should be established in an unequivocal and categorical way that the purpose of the incriminated transactions was not one's own enrichment, but an attempt to conceal the origin of the funds" whereas the evidence available in this case only indicates the desire of N. "*to get rich, and not to hide the origin of the funds*".

294. As result of this generally accepted interpretation, the offence in Art. 215 of the CC will serve as a remedy in cases the prosecution is unable to bring sufficient evidence for the subjective mental element (*mens rea*) of the ML offence. It remained unclear how often such changes in the criminal charges could have taken place in the assessed period, particularly as the offence of material concealment shows a rather moderate occurrence in the statistics, with 28 to 66 pre-trial proceedings initiated and 29 to 46 cases brought to court annually. On the other hand, however, the strictness of this judicial interpretation appears to go beyond what is required by the positive law (it refers to a mental element that cannot be found in Art. 253 CC) and may therefore pose another, unnecessary obstacle for the prosecution, as discussed more in details above.

295. The authorities also make frequent use of the non-conviction-based confiscation regime (see under IO.8) even if using such a mechanism would not by itself constitute a justifiable reason for not securing ML convictions in those cases.

Overall conclusions on IO.7

296. While the legal framework for the criminalization of ML includes almost all the material elements required by the standards, the successful investigation and prosecution of ML cases is hampered by various factors.

297. Bulgaria has a complex and sometimes redundant institutional framework for identifying and investigating ML activities, including various authorities with overlapping or competing competencies and repetitive proceedings. Many of the authorities (such as the AML Units within

MoI GDs) are impacted by the lack of sufficient staff with adequate expertise and limited technical resources.

298. In the pre-investigative operative proceedings, no sufficient attention is paid to examining the financial aspects of the proceeds-generating criminality and associated ML activities. The comprehensive understanding of the relevance of parallel financial investigations was not demonstrated in the pre-trial stage of proceedings either.

299. The overly high expectations of the prosecutors often result in rejection of the LEA referrals to for initiating formal pre-trial proceedings, which results in delays and loss of efforts. The extremely formalistic and bureaucratic features of the criminal procedure, particularly the strict and narrow deadlines, pose unreasonable obstacles for the authorities. ML is generally not considered a priority either by LEAs or the prosecutorial authorities.

300. The characteristics of ML offences investigated and prosecuted do not appear commensurate with the identified ML risks of the country. Most of the ML cases are related to proceeds of fraud and generated by the reporting regime, while there are hardly any ML cases involving proceeds of high-scale corruption or organised criminality.

301. The number of ML investigations and convictions in Bulgaria is generally low as opposed to the number of proceeds-generating offenders investigated and convicted. This can be attributed to the high evidentiary standards applied by the judiciary in ML cases, as a result of which stand-alone (autonomous) ML offences are absent from the Bulgarian criminal law.

302. The criminal sanctions imposed for ML are generally low, consisting of suspended imprisonment and moderate fines in most cases, often as result of an agreement concluded between the prosecutor and the defence. The calculation of criminal sanctions imposable for multiple crimes, as prescribed by the CC often results in associated ML charges being practically unpunished beside a more serious offence**.**

303. **Bulgaria is rated as having a low level of effectiveness for IO.7.**

3.4. Immediate Outcome 8 (Confiscation)

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

304. The complex system of the confiscation and provisional measures has not gone through any substantial changes since the adoption of the 2013 MER and therefore most of the technical deficiencies appear to prevail, which particularly refers to the rather limited scope of third-party confiscation and provisional measures together with other, less important technical shortcomings.

305. From a technical point of view, however, the regime for criminal confiscation as provided in Art. 53 of the CC and specifically under Art. 253 (6) for ML offences and Art. 108a (8) of the CC for TF, offers a relatively robust instrument for the authorities, particularly in relation to ML/TF offences where the general limitations to third-party confiscation do not apply.

306. As it is discussed more in details in the TCA, the system of provisional measures is rather complex in the Bulgarian law. The classic criminal coercive measures of search and seizure (Art. 109 of the CPC) only apply to objects representing material evidence, namely the (intended) instrumentalities as well as the subject (*corpus*) of the crime, or anything else that "*may serve to*

elucidate the circumstances in the case". While the latter term, on the face of it, appears broad enough to encompass almost everything that can be subject of confiscation under Art 53 of the CC (one could argue that criminal proceeds may also serve to "*elucidate*" the case) the Bulgarian law has another, specific measure for this purpose. It is a particular feature of the Bulgarian legal system that some of the provisional coercive measures available for seizing or freezing property in criminal proceedings can be found in the CCP (with a single connecting clause in Art. 72 of the CPC) and therefore civil precautionary measures are used for securing property, among others, for the purpose of criminal confiscation.

307. The combination of criminal and civil procedural measures does not appear to have caused any particular issues of effectiveness for the pre-trial authorities: as it was explained onsite, the court proceedings are timely in both regimes and *ex-parte* application of the measures is likewise provided for. Considering however the different approaches of the two, one can see a considerable overlap between their respective scopes (in terms of objects that represent material evidence and are subjects of confiscation too) which leaves room for some discretion by the prosecutor. In any case, the CPC rules can be applied in a broader scope (not only against the accused, and even before an accusation has taken place) and also in an urgent manner (without prior judicial approval) while the CCP measures can only be applied after a formal accusation has taken place, to any property item of the accused that is subject of confiscation but does not represent any direct material evidence.

308. In practice, proceeds of crime consisting of movable assets (cash, other valuables or vehicles) are seized pursuant to the CPC regime while immaterial assets (e.g., balance of a bank account) or real estate are secured by use of the CCP measures. Neither of these regimes appears to be applicable, however, for securing the entire spectrum of assets that can be confiscated under Art. 253 (6) of the CC, such as the object of the crime (the laundered property) if it is owned or held by third parties but does not constitute material evidence.

309. The other, more serious flaw of both regimes is the severe deadline in Art. 234 (8) of the CPC that significantly narrows down the effective applicability of all provisional measures. It provides that coercive measures taken in respect to the accused (thus including all CCP-based measures by virtue of Art. 72 of the CPC) cannot last longer than 18 months in case of serious crimes or 8 months in all other cases, after which all such measures must be revoked. ("Serious crimes" are defined by Art. 93 (7) of the CC as criminal offences for which the law provides for imprisonment of more than five years.) It goes without saying that the proper investigation of a serious proceeds-generating crime with OC and/or transnational implications, or a ML offence with complex laundering schemes, would easily and justifiably require more time than 18 months. Even in such cases, all seized property items must automatically be released, which may have a direct negative impact on the outcome of the criminal case. This unrealistically short deadline, as demonstrated by case examples, has frustrated the securing of criminal proceeds in high-scale criminal cases:

310.

Box 3.8: Example of revoking the precautionary measures due to expiration of the deadline

The main defendant was prosecuted for both the predicate crimes and associated ML. The predicates consisted of tax crimes committed in relation to fuel trade by evading VAT, excise duty, and corporate tax. The defendant purchased undocumented fuel from tax warehouses of distributors and producers, to which he added waste petroleum products and sold the product

as diesel fuel at commercial sites through his companies without issuing fiscal vouchers and without paying the due excise duty and VAT. He carried out this illegal activity for a period of several years, periodically changing the companies involved in the scheme, leading to non–payment of tax liabilities in especially large amounts.

As a result of this criminal activity, a sum of money in the total amount of BGN 2 763 052 (€1 412 195) was acquired. The defendant received the turnover from these unreported sales by hand, part of which in amount of BGN 1 533 077 (€783 850) he converted into euros and kept in a bank box in the name of a third party (another defendant in the case).

A thorough investigation revealed the ML scheme and attachment was imposed on the seized money as material evidence on €783 850 from the bank vault and BGN 24 600 (€12 577) from the home of the defendant. Seizure was imposed on a car type Mercedes-Benz ML 350 BlueTEC 4Matic, and other precautionary measures were imposed regarding receivables on the accounts of companies of the accused to ensure their confiscation. All these precautionary measures were, however, revoked on the grounds of Art. 234 (8) of the CPC, i.e. because of the expiration of the deadline, and the assets were released except for part of the seized cash, which was returned to a third person indicated by the court (the wife of the defendant).

311. As it was explained by representatives of the prosecution service, this strict and peremptory deadline, and the imminent risk to lose all secured proceeds before completing the investigation, is one of the main reasons why prosecutors often decide not to run against the clock (and to risk a premature indictment) and rather notify the CACIAF so as to initiate a non-conviction based civil confiscation procedure.

312. Indeed, the criminal confiscation regime is perfectly completed by the civil confiscation measures under the LCCIAF. The present, robust and autonomous mechanism for civil confiscation is a result of a gradual legislative development after two previous, now obsolete laws. In addition, there is a similarly CCP-based mechanism for securing property in the civil confiscation proceedings the applicability of which likewise requires an accusation and can only be applied regarding the property of the accused. While this procedure is apparently bound by a deadline of the same length as provided in Art 234 (8) of the CPC (maximum 1 ½ years that is 18 months) these two are not comparable because in this case, that period of time can entirely be dedicated for financial profiling and identification of criminal proceeds.

313. Despite several successful case examples, the Bulgarian law enforcement and prosecutorial authorities have not convincingly demonstrated that seizure of criminal proceeds and instrumentalities had been in the centre of their attention when pursuing proceeds generating crimes. As discussed already under IO.7, there appears to be no legal or other mandatory requirement to pursue confiscation as a policy objective (e.g., by routinely launching parallel financial investigations or analyses), the use of which is thus subject to discretion both in pre-investigative and pre-trial proceedings.

314. The lack of proceeds-oriented operative analysis in the pre-investigative stage has a direct impact on the effectiveness of any further measure to identify and secure proceeds in the pre-trial procedure. As noted under IO.7, such parallel financial examinations are very rare in the operative phase as most LEAs dealing with proceeds-generating crimes (with the probable exception of GD-COC) have neither time nor skills or experience to pay due attention to following the trail of money and identifying proceeds of crime. In an apparent lack of any target-oriented

supervision over the operative activities of the LEAs and without internal rules or methodologies to require exploring the financial aspects of a proceeds-generating crime or the financial profile of a perpetrator, any report the prosecutor will eventually receive for initiating a pre-trial investigation will necessarily be deficient in this aspect.

315. The situation is not much different in the pre-trial stage of proceedings, where no legislation or mandatory prosecutorial or other instrument defines under which circumstances and in what scope a parallel financial investigation should be carried out. The brief provision in Art. 102 (3) of the CPC according to which the "*family or financial status*" of the accused party should also be subject of proof in the criminal proceedings, cannot be considered sufficient in this respect. It is thus practically left to the discretion of the supervising prosecutor to decide whether and to what extent any investigative measures be taken to explore the financial aspects of the proceeds-generating crime and its perpetrator. The non-binding guidance available to the practitioners (see under IO.7) as it was described by the interlocutors onsite, appears to be a proper, although outdated, manual with relevance also in this field, but without any prescriptive character.

316. The AT were not provided with or informed of any strategy document or policy paper that would define asset recovery and the pursuance of parallel financial investigations as a priority requirement, except for the recently adopted Action Plan to the NRA (see below). It is thus no wonder that pre-trial authorities the assessors met onsite could not demonstrate comprehensively understanding the concept and importance of parallel financial investigations.

317. The case examples provided by the Bulgarian authorities do not imply the existence of any target-oriented approach in identifying and securing criminal assets. Only a handful of cases appeared to prove that the pre-trial authorities had put actual efforts in exploring the financial aspects of a proceeds-generating crime and thus identified not only the proceeds but the associated ML activities, such as in the following one:

Box 3.9: Case example of identifying the proceeds of crime and associated ML activities

The predicate offence was the crime in Article 252 (1) and (2) CC that is, carrying out banking transactions without permission and receiving significant illegal income therefrom (providing usurious loans to various individuals with extremely high interest rates). The total amount of the illegal income amounted to BGN 417 010 (€213 198) and the associated ML activity, which was prosecuted together with the predicate crime, consisted of converting these assets into other property by purchasing real estate.

A wide range of various investigative actions were carried out, such as hearing of witnesses (incl. victims), use of various forensic experts (IT/technical, psychiatric, medical, graphic, accounting). performing search and seizure in 10 premises, obtaining banking and other documentation, and use of data from available databases.

By a decree of the supervising prosecutor, precautionary measures were imposed on the defendants by seizure of various movables, bank accounts, cash receivables and foreclosure of real estate owned by them, in their capacity as individuals and owners of commercial companies. The case is pending before the court.

318. A logical explanation for the moderate occurrence of such cases among the examples and, more generally, for the lack of awareness regarding parallel financial investigations is the

extensive use of the civil confiscation proceedings by the CACIAF as an alternative to pursuing criminal proceeds in the criminal proceedings. As it will be discussed below, the civil confiscation regime has demonstrably been utilised in the assessed period with a notable level of frequency and apparent effectiveness. The CACIAF has a dedicated staff for asset identification and recovery with skills and experience as well as with external expertise if necessary. No issues of human or financial resources were mentioned by CACIAF representatives onsite, which is appreciable even if the AT harbours some doubts whether the gradually extending competences of this Commission (asset recovery office, asset management office and anti-corruption agency at the same time) will eventually have a toll on this ideal situation. The CACIAF asset identification procedure is to a lesser extend bound by time constraints and the civil confiscation mechanism is entirely separate from the criminal proceedings.

319. It thus comes as no surprise that prosecutors burdened with the formalities of the criminal procedure willingly "outsource" the financial investigative tasks to the CACIAF leaving them with all responsibility to identify, to secure and to confiscate criminal proceeds particularly in the most complex (and thus the most time consuming) cases. This approach, however, has its disadvantages also. The autonomy of the civil confiscation procedure means that once the prosecutor notifies the CACIAF of a person having been accused of a serious crime, any result the examination of his property profile yields will only be used for the purposes of civil assets recovery and confiscation, with no apparent feedback to the prosecutors. When identifying the property of the accused, the CACIAF inspectors would focus on the assets and not on the associate money laundering activities performed by either the accused or a third person. Another deficiency of this mechanism is that it does not extend to assets held or owned by third persons (as opposed to the criminal confiscation measures for confiscating proceeds of crime and the object of the ML offence).

320. Furthermore, from a methodological point of view, the CACIAF civil confiscation procedure, however effective it is, cannot be considered being compatible with the FATF standards regarding the confiscation of criminal proceeds, instrumentalities or the property laundered. The mechanism operates entirely separately from the criminal procedure, regardless whether the accused will eventually be indicted at all, and extends to all his unexplainable property without any distinction. As a result, the civil confiscation being a perfect complementor for the conviction-based confiscation mechanism, it should nevertheless not be considered as its substitute.

321. Another part of the cases is where provisional measures and confiscation take place as result of postponement of a suspicious transaction by the FID-SANS, as illustrated by the Table 3.18 below:

Table 3.18: Provisional measures and confiscation as result of postponement of a suspicious transaction by the FID-SANS

Year	Number of postponement orders issued by the FIU[43]	Number of cases where the postponement was followed by a preliminary	Number of cases ended with an indictment	Number of cases ended with a conviction and confiscation

[43] See also Table 3.7 under IO.6. One order might refer to more than one transaction.

		investigation and a freezing order was issued		
2014	5	5	-	-
2015	11	10	-	-
2016	19	12	1	-
2017	6	6	-	1
2018	12	12	1	-
2019	41	36	(no figures provided)	
2020	73	73		
2021 (01-07)	17	17		

322. Although the Table 3.18 above only covers the first part of the assessed period and some relevant figures are entirely missing (such as the volume of assets seized and confiscated) it can be concluded with certainty that while the prosecution in the majority of the cases agrees with the FIU and proceeds with the freezing order, these cases will very rarely be prosecuted and brought before the court, most likely because of the premature stage of the cases at the time they are being reported to the prosecutor.

323. There is a clear mechanism in place for managing and/or disposing of property subject of security measures in a criminal procedure, with the prosecutor's offices and the CACIAF being in charge of handling such property. This activity, however, does not extend beyond storage and safekeeping measures which has a direct impact on effectiveness, particularly if more complex types of assets must be managed. Furthermore, there is no specific mechanism available for managing and disposing of property that has been confiscated under the CC.

324. Movable property items that constitute material evidence in criminal proceedings are kept by the competent prosecutor's office pursuant to the detailed rules for keeping material evidence (Regulations for the administration of the prosecution in the Republic of Bulgaria, Chapter Five). For this purpose, all prosecutor's offices have specific bank accounts (in different currencies), special safety boxes in banks, and special rooms for storage of material evidence, as well as appointed employees who are responsible for that safekeeping. In case a property item subject of security measures is not (or has ceased to be) considered material evidence in the criminal proceeding, it will be managed by the CACIAF upon notification of the prosecutor.

325. However, this was not always the case. In the first part of the assessed period (until July 2019) the management of assets seized by the court was in all its aspects controlled by the competent supervising prosecutor and implemented by a civil enforcement agent (bailiff). Upon receipt of a ruling from the court under Article 72 CPC on issuing a precautionary order under the Civil Procedure Code, the prosecutor sent these documents to the bailiff who performed inventory, assessment, and transfer of the movable property for safekeeping, and the imposition of foreclosure on real estate by entering the court's security order in the land register.

326. The new Art. 72a of the CPC being in force since July 2019 rules that property secured under Art. 72 CPC (with the exception of assets securing the fine) is to be managed and protected by the CACIAF pursuant to their respective legislation, which is the Rules for interaction between the Prosecutors' Office of the Republic of Bulgaria and the CACIAF (No. 1186 of 22.11.2019)

implemented for the Prosecutor's Office by a special order of the Chief Prosecutor (RD–04–416 dated 05.12.2019).

327. When, at the request of the prosecutor, the court imposes a security measure pursuant to Art. 72 of the CPC, the prosecutor not only notifies the bailiff thereof, but also sends copies of all documents to the CACIAF, which then proceeds for securing all movable and immovable property items through the bailiff, as above. Such notifications took place 19 times in 2019, 76 times in 2020 and 15 times in the first half of 2021, which indicates the number of underlying criminal proceedings. The CACIAF then periodically (on an annual basis) notifies the prosecutor on how and where the property seized in the case is being kept and managed.

328. The instructions the prosecutors give to CACIAF mainly extend to releasing the detention of the property if the legal basis has disappeared or to notifying the CACIAF that the case has been filed in court (although the prosecutor can also give instructions regarding the relocation and other disposal of the seized items if necessary).

329. As it was clarified onsite, the CACIAF competence only extends in practice to the storage and safekeeping of the secured movable property items (which in most cases means vehicles) that need to be properly stored so that they keep their value. As a main rule, this is carried out by the CACIAF itself, through a separate structural unit, which is also responsible for regularly checking the condition of the seized vehicles. Certain categories of movable assets are submitted for safekeeping to various bodies according to Art. 162 of the LCCIAF (e.g., movables of historical value to the National History Museum or another museum, movables made of precious metals or stones to the BNB etc.) The secured funds, as well as those from the sale of movables, are deposited in special bank accounts of the CACIAF with the BNB.

330. No specific safekeeping mechanism (rules and measures) are in place, however, for preserving the value of secured real estate. Specifically, there appear to be no specific mechanisms available for actively managing and thus preserving the value of complex assets belonging to and being used by a business entity, such as a real estate used for business purposes or a set of movable items constituting accessories of a functioning business entity (e.g., a hotel or a restaurant with its respective equipment). In such cases, the safekeeping of those assets in itself would not compensate for the loss of value caused by the interruption of the business and could only be maintained by running the business entity during the security measures. Instead of that, the CACIAF would only enter the foreclosure on the respective real estate (e.g., the hotel) in the registry and have the bailiff to make an inventory of all movable items (e.g., the equipment of the hotel) which would then be transferred for safekeeping, with the exception of perishable items, which could be sold in advance, pursuant to Art. 163 of the LCCIAF (carried out by a bailiff in a procedure that is subject to judicial control). As a result, the business entity would effectively be wound up and eventually sold by its components.

331. Statistics available on all property secured in criminal proceedings and managed (kept) by the CACIAF from 2015 to 2021 (which must be to some extent inaccurate since Art. 72a of the CPC has only been in force since 2019) shows that most of these property items were vehicles (164 in the entire period out of which 142 cars) and cash (more than € 3 500 000 throughout the period). There have been 79 various real estate, consisting mostly of apartments, lands, and similar property items, but none specifically related to business (no industrial buildings or tourist or social facilities etc.). The prosecutorial statistics on seized assets (see below), however, indicate that business entities have already been secured (e.g., a commercial building and a warehouse in 2020) which means that the CACIAF must have already encountered the problem

described above. No statistics were available on specific property items in the safekeeping of other bodies (e.g., the BNB).

332. Both the pre-trial authorities and the CACIAF appear equally incapable to effectively secure, manage and recover virtual assets (e.g., Bitcoin). The interlocutors met onsite were unsure exactly how the decision on seizure, confiscation and thus the appropriation of a cryptocurrency would be executed and indeed, it has never happened in practice. On the other hand, crypto-currencies appear to occur in criminal cases as means of criminal proceeds (the selected case examples provided by the authorities contain several such cases) which would require urgent steps from the authorities' side both in terms of establishing the necessary technical and legal framework for the seizure and confiscation of crypto-currencies and providing adequate training to all stakeholders involved.

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

333. As noted above, the AT was not made aware of any strategic document specifically dealing with the confiscation of proceeds and the related parallel financial investigations. The lack of strategic planning in this field may easily be a direct consequence of the fact that Bulgarian authorities apparently have zero statistical information on the functioning of the criminal confiscation and provisional measures mechanism, including even the most basic performance indicators.

334. When assessing the effective functioning and the output of the confiscation regime, the AT need to consider a variety of facts and data, a relevant part of which, however, in most cases consists of numeric information indicating the performance of the regime as well as any changes or trends that have occurred in that field throughout the assessed period. This numeric information is usually provided to the assessors in the form of statistical tables, regardless of whether the given jurisdiction does keep and maintain statistics in that particular matter (which is of course the preferable way) or the respective figures were only gathered in that format for the sake of the assessment. In lack of statistical or at least numerical figures, an approximate estimation by the competent authorities can also be taken as a ground for drawing conclusions.

335. In any case, the onus to demonstrate the effective performance of the confiscation and provisional measures regime, either by statistical figures or by any other numeric or measurable means, is always on the assessed country. The AT needs to conclude at this point that in case of Bulgaria, this requirement was met only to a very limited extent. In respect of the performance of the civil confiscation regime, the assessors were provided with proper, although not too detailed, statistical figures by the CACIAF, and the same goes for figures on assets seized in pre-trial proceedings provided by the prosecutors. On the other hand, however, the AT were not provided with any numeric information regarding even the most basic features of the system for criminal confiscation, claiming that the official statistics do not contain such information. As a result, the authorities were unable to specify:

(i) in how many cases criminal confiscation (Art. 53 of the CC) was applied in the assessed period, both in general terms and broken down by the relevant criminal offences (ML, TF, predicates)
(ii) the volume/amount and typical characteristics of property confiscated in the assessed period (indicating annual aggregate figures for the volume as a minimum)
(iii) the volume of property that has not only been confiscated but also successfully recovered.

336. Furthermore, neither the prosecutorial statistics on seized assets are sufficiently detailed, as they focus on the assets themselves while do not contain sufficient information on the characteristics of the underlying criminal proceedings (i.e., what the respective criminal offence was in those cases). As a result, the assessors could not draw conclusions as to the actual volume and performance of the criminal confiscation and provisional measures regime, let alone assessing the ratio between the volumes of assets seized/frozen, confiscated, and recovered; or identifying and analysing any specific features or upwards/downwards trends in this field. In other words, the AT can only conclude that Bulgaria has not demonstrated to a sufficient extent that the criminal confiscation and provisional measures regime is performing with adequate effectiveness. But again, the lack of statistical information in this respect indicates a more generic problem - namely the likely possibility that not only the assessors, but also the Bulgarian authorities themselves have no actual insight into the size, the characteristics, and the performance of this regime, which may prevent them from identifying and eliminating the various flaws of the mechanism.

337. The prosecutorial statistics on assets seized in pre-trial proceedings indicate hardly any notable seizures until 2018. According to the statistics, there were absolutely no security measures imposed in 2015 and generally very few between 2014 and 2017 (seizures being applied in one single case for 2014 and in 4 cases for 2016 and 2017) involving a limited number of real estate and a more significant number of bank accounts but without indicating any actual value.

338. The number of cases with asset seizures started to increase from 2018 (with 5 cases per year for 2018 and 2019, 14 for 2020 and 7 for the first half of 2021) together with an increase in the number and value of assets involved. Statistics for 2019, for example, indicate a case where more than € 258 000 EUR worth in cash and € 540 000 in bank deposits were secured together with a real estate. In 2020, the statistics show numerous cases where various forms of real estate were secured (from 2-floor buildings to warehouses and farmlands) some others with the seizure of several cars (96 and 54 respectively) as well as 2 280 pieces of cultural and historical properties or almost € 5 000 000 deposited in bank accounts.

339. While the general increase in the figures and the occurrence of significant property items in the statistics for the last 3 years unquestionably demonstrates an enhanced awareness and increased effectiveness on the side of the pre-trial authorities, the large picture remains ambiguous. The number of cases where assets are seized in pre-trial proceedings are still dwarfed by the overall number of pre-trial proceedings in Bulgaria (see under IO.7) which means that such provisional measures are only applied in a fragment of the cases. Furthermore, there is absolutely no information available regarding what proportion of these seized assets will eventually be subject of confiscation (and not released e.g., because of the expiration of the deadline in Art. 234. [8] of the CPC).

340. The total lack of statistical information on (conviction-based) confiscation could only partially be remedied by case examples intended to illustrate the effective application of the confiscation measures. In the selected cases, which were all related to the ML offence, conviction-based confiscation measures based on the specific provision in Art. 253 (6) of the CC were applied with regularity. On the other hand, the rather simple characteristics of the underlying cases (ML consisting of withdrawal of a sum of money, or purchase of a vehicle or real estate with the money derived from one's crime) resulted in equally simple confiscation orders (limited to the sum of money withdrawn or to the vehicle purchased by proceeds).

341. The case examples nevertheless demonstrated that confiscation of the equivalent value as well as third-party confiscation under Art. 253 (6) of the CC are equally applied by the courts which also proves that the prosecution in those cases was successful in maximising the opportunities offered by the legislation (the lack of third-party confiscation in the general regime is a technical shortcoming that has direct implications on the effectiveness as well). Neither the case examples, nor the interviews conducted onsite indicate that proceeds of domestic criminal offences that can be found abroad have ever been subject of any successful confiscation measure (either conviction-based or civil).

342. As noted above, the only comprehensive statistics the AT was given in relation to IO.8 had been provided by the CACIAF to demonstrate the performance of the civil confiscation regime as follows:

343. **Tables 3.19:** Measures applied by CACIAF based on civil confiscation regime

Year	Property seized / frozen		Property confiscated		
	type	quantity / value	type	quantity	value
2015	real estate	80 items	real estate	38 items	
	vehicles	44 items	vehicles	19 items	
	financial assets, shares and gold	171 items	financial assets		€1 178 512
	Total amount[44]: €724 629 468		**Total amount**: €3 299 719		
2016	real estate	151 items	real estate	277 items	
	vehicles	76 items	vehicles	56 items + 1 boat	
	financial assets, shares and gold	79 items	financial assets		€1 950 737
	Total amount: €5 398 744		**Total amount**: €9 599 144		
2017	real estate	474 items	real estate	131 items	
	vehicles	799 items	vehicles	57 items + 1 boat	
	financial assets, shares and gold	42 items	financial assets		€7 190 716
	Total amount: €111 305 512		**Total amount**: €14 209 675		
2018	real estate	467 items	real estate	84 items	
	vehicles	1034 items	vehicles	27 items + 1 boat	
	financial assets, shares and gold	61 items	financial assets		€5 130 570
	Total amount: €20 114 993		**Total amount**: €6 698 239		
2019	real estate	1509 items	real estate	37 items	
	vehicles	615 items	vehicles	119 items	
	financial assets, shares and gold	112 items	financial assets		€2 820 320
	company shares	20.000 items			
	Total amount: €288 744 651		**Total amount**: €4 178 101		

[44] Including other assets not specified in the table (such as funds on bank accounts or in bank safety boxes).

2020	real estate	369 items	real estate	43 items	€1 102 965
	vehicles	340 items	vehicles	550 items	€635 724
	machinery, equipment	4 items	receivables		€4 623 182
	gold, items of historical or scientific value	€32 383 602			
	securities	€343 843			
	company shares	€2 918 870			
	receivables	€888 095			
	financial assets	€3 190 028			
2021 (01-07)	real estate	138 items (Σ: €7 219 375)	real estate	6 items	€383 858
	vehicles	779 + 1 boat (Σ: €1 904 102)	vehicles	9 items	€61 048
	machinery, equipment	1 item	gold, items of historical or scientific value		€2 639
	gold, items of historical or scientific value	€512 905	receivables		€1 050 886
	company shares	€1 088 099	financial assets		€28 369
	financial assets	€173 185			

344. The figures in the Tables 3.19 above on property seized, frozen and confiscated are impressive and demonstrate the efforts the inspectors of the CACIAF had put in exploring and identifying the property status of individuals having been accused with serious offences (regardless of the outcome of the criminal proceedings). The statistics kept by the CACIAF, however, do not allow for a more profound analysis in lack of data regarding in how many cases (against how many individuals) these measures were taken and what the respective criminal offence was with which these individuals had been accused (e.g., what proportion of the measures indicated in the above statistics had originally been related to ML/TF, OC and corruption.) Trends or tendencies in the Tables 3.19, however, do not need to be specifically analysed considering that the CACIAF has no proactive role in identifying their respective targets as the scope of their activities is entirely determined by what notifications they receive from the prosecutors.

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

345. As discussed under C.32.8, the technical side of the cross-border cash control regime is partially incomplete due to the lack of domestic legislation to provide for a legal framework for stopping and restraining cash/bearer negotiable instruments (BNIs) transported through the internal borders of the EU.

346. The measures to detect illegal physical transport of cash/BNIs are generally present at the EU external borders of Bulgaria (those with Serbia, Northern Macedonia, and Turkey as well

as the international airports in Sofia, Varna, Burgas, Plovdiv and the ports of the Black Sea and the Danube, and to a certain extent also on the EU internal borders. Such control measures are performed by the National Customs Authority based on risk analysis by targeted selection of individuals representing the risk. This is mainly carried out by ad hoc profiling of the persons against indicators such as the amount of money transported (if declared), the route of the person, the occurrence of any previous non-declaration and the respective modus operandi. This analysis is assisted by an automated system that has been in place since August 2021 into which all cash/BNI declarations are entered as well as identified false or non-declarations, upon which data the system performs a risk analysis. The same module is used for EU external and internal borders alike (the declaration forms are different in the two regimes, but the contents are practically the same) although it is mostly used for processing declarations at the external borders.

347. This module being quite a recent development, its functionality could not yet be assessed. (The previous system being in place until August 2021 did not have a risk analysis feature.) The Customs authorities the team met onsite admitted that entering all the necessary data into the module used to take a long time (mostly because all declarations are submitted on paper) but now it is not more than 5 minutes per person. The module is linked with the database of Bulgarian ID documents (equipped with ID readers to facilitate the insertion of data into the system) and the commercial register, but not connected to the criminal register and the register of bank accounts which, in the view of the AT, would be equally important for the purposes of risk analysis.

348. Notwithstanding all these, the actual results are rather moderate, both in general terms and in relation to cash/BNIs suspected to have been derived from criminal activities. The Table 3.20 below summarizes the incoming/outgoing declarations as well as the few cases of false or non-declaration of cash/BNIs that have occurred throughout the assessed period.

349. **Table 3.20: Cross border transportation of currency and bearer negotiable instruments**

Year	Number of declarations and disclosures		Suspicious cross border incidents			Assets restrained (€)
	Incoming	Outgoing	Suspicion of ML*	Suspicion of TF	False / non-declaration	
2015	986	173	9	0	39	1 993 438
2016	751	174	8	0	37	1 971 502
2017	820	163	5	0	35	1 931 917
2018	885	184	5	0	28	1 072 088
2019	977	226	5	0	45	2 008 906

2020	448	82	3	0	27	1 006 391
2021 01-07	308	52	6	0	23	3 364 035

* *number of all notifications for suspicious operations sent by the Customs Authority to FID-SANS*

The vast majority of declarations/disclosures involved currency in cash, with only a sporadic occurrence of BNIs which are therefore not indicated separately in the Table 3.20. The number of incoming currency declarations/disclosures is remarkably higher, which appears to indicate that assets earned abroad, typically by the Bulgarian diaspora residing and working in Western Europe, are mostly transported back to Bulgaria for purchasing property (such as real estate). Assets restrained indicate the total amount of falsely or not disclosed monies as established by the Customs Authority, which were released and returned after the payment of the fines imposed.

350. As regards violations and sanctions, the authorities provided more detailed figures for the years 2019 and 2020 as follows in Table 3.21 below:

351. **Table 3.21:** Violations and sanctions

	Administrative Offences		**Art. 251 CC**
	Fines for non- declaration	**Undeclared cash confiscated**	**Fines**
2019	∑ 3580 € (in 7 cases)	∑ 84.533 € (in 5 cases)	∑ 131.793 € (in 6 cases)
2020	∑ 61.489 € (in 47 cases)	∑ 40.600 € (in 2 cases)[45]	∑ 40.685 € (in 2 cases)

352. As it was explained, these figures are not compatible with those in the Table 3.21 above because of the different methodologies applied (data in this table only refer to violations occurred in the given year, but also include confiscations in cases where the offender remained unknown.) Regardless of any methodological differences, though, these figures appear extremely low in comparison to those in the previous table and thus corroborate the concerns discussed above.

353. The NCA is authorised to perform pre-investigative proceedings in relation to a number of cross-border criminal offences (including smuggling, tax evasion or failure to declare the transport of cash or precious metals) and administrative offences, and also to do operational search activities with the purpose of detecting crime. The NCA is assisted in their cross-border duties by the Border Police which, apart from their tasks in the physical protection of the state border, also perform pre-investigative proceedings in relation to all crimes with cross-border characteristics, often in joint operation with the NCA. As the Border Police are not constantly

[45] As from February 2020, the undeclared and seized cash is no longer subject of criminal confiscation.

present at the EU internal borders, they set up joint mobile operative teams there with the NCA to identify the potential targets.

354. The operative activity of the NCA and the Border Police, however, does not extend to ML/TF which crimes clearly fall beyond their powers and thus are not among their targets. As a result, when it comes to the phenomenon of cross-border physical transport of cash or BNIs, the main focus is on the respective administrative offences, and the only criminal offence the occurrence of which is actually considered both by the Customs and the Border Police is the failure to fulfil the obligation to declare cash or precious metals and stones, in particularly large amount, at the external borders of the EU (see Art. 251 CC). The operative proceedings, including the risk analysis and the profiling of the potential perpetrators, are mostly targeted at this specific criminal offence, and this is the very crime that in most cases will eventually be reported in practice to the competent prosecutor for considering the initiation of a pre-trial investigation.

355. Consequently, ML suspicion has only been detected in a limited number of cases by the NCA which were then reported to the FID-SANS even though all occurrences of undeclared cash with unknown source of funds, as it was explained to the AT onsite, should theoretically have been reported as a ML suspicion. As discussed under C.32.8, Art. 7 of the 2018 EU Regulation provides, that competent authorities may also detain cash/BNIs if there are indications that it is related to criminal activity. This rule is directly applicable in Bulgaria since 3 June 2021 but had not yet been applied by the time of the onsite visit. As the competent Bulgarian authority, the NCA has thus not demonstrated its capacity to detect and to restrain ML/TF related cash/BNIs while the few cases of false or non-declarations have reportedly had no ML/TF implications.

356. In contrast, at least one significant ML case has reportedly been detected and reported by the Border Police, which is currently in pre-investigative phase, although proving the ML offence appears to be challenging due to the high evidentiary standards regarding the predicate offence (as discussed under IO.7).

Box 3.10: Case example demonstrating high evidentiary standards regarding the predicate offence

A Chinese citizen with a permanent residence in Spain transported a sum of cash in the amount of 704,000 EUR on 20.08.2019 across the border of the country at the Sofia Airport upon her arrival from Spain. This individual was expected at the airport by Chinese citizens residing in Bulgaria. The individual did not declare the cash she carried. The Border Police intervened and searched the person, as a result of which the sum of cash was found and seized.

No immediate explanation was available to the origin of the money which was therefore presumed to be derived from crime. A pre-trial investigation for ML was initiated by the competent prosecutor's office. In order to establish the predicate offence, the assistance of the Spanish authorities was requested through the EUROJUST, as a result of which detailed information was obtained on the property profile of the Chinese individual and her related persons. Information received through police channels indicated that one of these persons was investigated for ML in France. Various other investigative measures were taken (including seizure of video evidence, issuance of EIOs, obtaining data on mobile phone and internet communication which show that the amount transferred was part of remittances sent through couriers engaged for a fee, such as this Chinese citizen, who had regularly travelled from Spain to Bulgaria and back. The money was sent by Chinese citizens operating in Spain to various countries in Europe, but the reason for choosing this way of transferring the money, as well as the actual source of the funds, have not yet been established. All information has been brought to the attention of Europol.

The investigation is currently ongoing, with efforts aimed at gathering evidence of the origin of the incriminated funds and their possible connection with crimes committed in Spain or France.

357. Notwithstanding that, the AT has serious concerns about the ML/TF awareness of the NCA and the Border Police in general, which substantiates the risk that some of the cases where the offence in Art. 251 of the CC (or, below the threshold of "*particularly large amount*", the respective administrative custom offence) was detected, would actually have qualified as ML considering that the concealed (non-declared) cross-border transportation of a sum of cash can in itself raise the suspicion of ML (which, on the other hand, also raises some questions about the ML/TF awareness of the prosecutors supervising the respective investigations for the offence in Art. 251 of the CC).

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

358. As discussed in IO.1, the main threats for ML indicated in the NRA were the high-scale corruption and organised criminality (particularly a number of trafficking offences) together with other, somewhat less serious predicate offences such as tax crimes as well as computer and social engineering fraud. It could not however be established with certainty whether and to what extent these criminal offences had directly or indirectly (i.e., as predicates to ML) been represented among the cases where provisional measures or confiscation (either criminal or civil) were applied in Bulgaria, due to the absolute lack of statistical figures mentioned above. In any case, the numerous ML-related case examples provided by the authorities represented several confiscations applied in fraud-related ML-cases and a couple in OC related cases (a successful case in a ML case related to usury is referenced above).

359. The main ML vulnerability identified in the NRA with a direct impact on the confiscation and provisional regime was that parallel or subsequent financial investigations had not at all been performed or were only conducted at a much later stage when the assets could not already be secured and confiscated. This was attributed to other vulnerabilities, such as the insufficient awareness of the LEAs and the lack of a proper practical methodology/guidance for conducting financial investigations.

360. While the AT gives credit to the authorities for having recognized shortcomings in this area, no efforts appear to have since taken in the field of policy making and issuing adequate methodological guidance to the practitioners until the recent Action Plan to the NRA. The actions contained in this document include the development of methodologies/guidance for financial investigations, containing standard materials and detailed legal procedures that have to be followed in cases of proceeds generating crimes as well as for the establishment of illegally acquired assets, and also concerning operations with VCs, both scheduled for June 2022.

361. As a result, the AT could not establish whether confiscation results were consistent with ML/TF risks identified and that the performance of the entire confiscation regime was in line with national AML/CFT policies and priorities.

Overall conclusions on IO.8

362. The rather complex and generally robust system of confiscation and provisional measures in Bulgaria (including the civil confiscation regime) suffers from technical flaws, the most serious of which is the limited scope of third-party confiscation and seizure/freezing which is only provided for ML/TF offences.

363. All provisional (precautionary) measures applied in the pre-trial proceedings are constrained by strict and narrow deadlines which frustrates the securing of criminal proceeds in high-scale criminal cases.

364. Provisional measures to secure property subject to confiscation are only taken in a very limited number of pre-trial proceedings.

365. There is no law or any other instrument to require pursuing confiscation as a policy objective (e.g., by routinely launching parallel financial investigations or analyses). The use of such measures is therefore entirely subject to discretion of the authorities.

366. Absence of statistical figures or approximate estimations in this field completely impeded the assessment of the performance and effectiveness of the criminal (conviction-based) confiscation regime and the recovery of confiscated assets.

367. The technical side of the control regime for cross-border transport of cash/BNI is partially incomplete in lack of the necessary domestic legislation, as a result of which there is no legal framework for stopping and restraining cash/BNIs transported through the internal borders of the EU. The National Customs Authority has not demonstrated its capacity to detect and to restrain ML/TF related cash/BNIs.

The active management of seized/frozen assets beyond storage and safekeeping measures is not provided for, and the same goes for managing and disposing of property that has been confiscated. All authorities appear equally incapable to effectively secure, manage and recover virtual assets (cryptocurrencies) although such assets frequently occur in case practice

368. **Bulgaria is rated as having a low level of effectiveness for IO.8.**

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

a) The perception and understanding of TF related risks by the competent authorities is generally uneven and limited, failing to adequately address all characteristics of potential TF activities in the country and the region, which particularly refers to risks related to the financial and non-financial system.

b) Generally low understanding of the TF risks by FIs and DNFBPs results in low-quality of TF-related STRs which in turn generate low-quality FIU disseminations with little added value.

c) Bulgaria does not have a national CT or CFT specific strategy, instead of which CT (and to a lesser extent, CFT) elements are included in more general strategies. It was not demonstrated that TF investigations were integrated with or supported those strategies (as it was the case with the NRA). Outcomes of terrorism-related criminal proceedings are not sufficiently used for domestic and UN designations.

d) The authorities involved in the operative analysis, criminal investigation, and prosecution of terrorism-related and TF cases generally demonstrate adequate specialisation, experience and expertise resulting in good cooperation in, and proper prioritization of such cases.

e) A limited number of terrorism-related offences have been prosecuted and some have already resulted in successful convictions, but no prosecutions and convictions of TF offences have taken place in Bulgaria with only 2 TF cases being investigated in pre-trial proceedings. Although one of these cases demonstrated the authorities' capability of prosecuting complex TF structures, the investigating and prosecuting authorities did not generally demonstrate to have an effective and systematic approach to explore and investigate the financing aspects of the terrorism-related offences occurred.

Immediate Outcome 10

a) Bulgaria implements the United Nations Security Council Resolutions (UNSCRs) 1267/1989, 1988 and 1373 without delay through a combination of supranational and national mechanisms. The Ministry of Foreign Affairs (MFA) is the central authority vested with powers of transposing UNSCRs through publishing them on its website, after which they become part of national legislation and thus are binding for all natural and legal entities.

b) Bulgaria has not proposed or made any designations pursuant to UNSCR 1267. Bulgaria has demonstrated a practical implementation of the UNSCR 1373, although it must be stressed that the results of recent terrorism related criminal proceedings

are not sufficiently used for domestic and UN designations. There are no mechanisms and publicly known procedures in place for delisting individuals or entities and unfreezing of assets with regard to UNSCRs 1276 and 1988 and there was confusion among the competent authorities to whom such requests should be sent.

c) Deficiencies exist in the immediate communication of the UNSCRs to competent authorities and OEs. The process of communication is not done in a constant and timely manner, which could hinder the effective implementation of UNSCRs, particularly in case of the FIs and DNFPBs that do not rely on automated sanctions screening mechanisms (as has been analysed in IO.4).

d) Although no assets have been identified and frozen pursuant to the sanctions regimes under UNSCR 1267/1989, 1988 or 1373, OEs demonstrated awareness of the targeted financial sanctions (TFS) regime, that is evidenced by identifying false positive matches to the lists.

e) Bulgaria has not conducted a proper and thorough TF risk assessment of its NPO sector. The NRA contains some analysis on the NPOs as a sector being vulnerable to TF abuse, however, the data collected for the purposes of TF risk assessment does not amount to comprehensive analysis on the activities and vulnerabilities of NPOs. The need for further comprehensive sectorial risk assessment for determination of the TF abuse risk was highlighted by the authorities.

f) Bulgaria has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs. However, neither the legislative measures in place, nor the monitoring and or supervision is risk based. The latter are applied regardless of TF risk to all NPOs operating in the country. The supervision of NPOs does not consider the results of NRA or other TF-related risk assessments. A number of outreach and educational activities were provided to the sector specifically targeting the risk of TF abuse. The NPO sector has a general understanding of TF risks and their respective obligations.

g) No assets have been frozen pursuant to the sanctions regime under UNSCR 1267/1989 and 1988. Bulgarian authorities and the OEs met on-site confirmed that if funds or other assets are identified, these would immediately be frozen. As indicated under IO.9, the investigation of the financial aspects of the relatively few cases related to terrorism appears not to take place as a policy, which hampers also the effectiveness of deprivation of TF-related assets and instrumentalities by LEAs.

h) There are several factors that hamper the implementation of the TF-related TFS in line with the overall TF-risk profile. These factors are related to the comprehensive understanding of TF-risks, including the NPO sector.

Immediate Outcome 11

a) Bulgaria implements proliferation financing (PF) related TFS through EU regulations and thus is generally impacted by the delays between the designation decision taken by the United Nations Security Councils (UNSCs) and its transposition into the EU framework. According to the authorities the general legal framework (in particular, the Constitution and the Act on International Agreements) gives the ability to the Council of Ministers to overcome the delay and transpose the UNSCRs directly.

Nevertheless, the mentioned legal provisions were not tested in practice during the assessed period.

b) Bulgaria has a robust export control regime to mitigate the risks in relation to proliferation (P). The activities *per se* also include PF issues, including checks against UNSCR related to PF. The FID-SANS proactively exchanges information with specialized directorate within SANS in relation to granting licenses for dual use or sensitive goods, or import, export activities which raise proliferation related suspicions providing information in relation to the financial aspects.

c) Measures taken by the OEs in relation to TFS to combat PF do not differ from those to combat TF. All FIs and DNFBPs lack a comprehensive understanding of PF-related obligations, and consider they are equal only to the screening with the relevant lists.

d) Supervisory authorities do not have legally defined powers to supervise and sanction TFS obligations in relation to PF, however, as they stated they check the compliance of OEs with sanctions screening obligations, which *per se* include PF-related UNSCRs.

e) No specific guidance has been provided to OEs on obligations in relation to TFS for PF and relevant sanctions evasion techniques.

Recommended Actions

Immediate Outcome 9

a) Bulgaria should conduct more comprehensive assessment of national TF risks in all its aspects (and particularly in the financial and non-financial systems of Bulgaria) to strengthen the understanding of TF risks and improve in TF investigations and prosecutions.

b) The FID-SANS needs to enhance its in-depth analysis of TF-related STRs to produce disseminations of a higher quality. For that the FID-SANS needs to be provided with sufficient resources to enhance its expertise.

c) Bulgaria should issue a national strategy specifically on CT and CFT related issues, making extensive use of the results stemming from pre-investigative proceedings and criminal investigations of such activities in the country.

d) Bulgaria should ensure (e.g., by means of instructions to pre-trial authorities) that detection and investigation of all financing aspects are carried out in a systematic manner for all terrorism-related offences extending, parallel to the investigation of the terrorism case, to all forms of TF and including investigating the sources of travel or subsistence costs of foreign fighters.

Immediate Outcome 10

a) Bulgaria should enhance its communication mechanisms and proactively communicate all newly adopted and amended UNSCRs to all competent authorities and OEs in a timely manner.

b) Bulgaria should expand the use of outcomes of terrorism related criminal proceedings for domestic and UN designations.

c) Bulgaria should urgently develop adequate mechanisms and procedures for delisting and unfreezing with regard to UNSCRs 1276 and 1988.

d) Bulgaria should urgently conduct an in-depth risk assessment of the NPO sector to form an objective analysis of risks posed by the sector based on underlying comprehensive assessment of all characteristics and statistics to identify those NPOs at risk from terrorist abuse.

e) Bulgaria should implement targeted supervision or monitoring towards those at risk in the NPO sector, without hampering legitimate NPO activity.

f) Bulgaria should enhance the outreach and provide relevant guidance to NPOs with a particular focus on TF risks and relevant NPOs obligations, as well as continue encouraging NPOs to use regulated financial channels. Specific outreach activities should be provided also to the donor community, with a focus on end use of NPO funds.

Immediate Outcome 11

a) Bulgaria should ensure that PF-related TFS are implemented without delay.

b) Bulgaria should expand the scope of national mechanism to combat proliferation or introduce a separate PF dedicated mechanism for the coordination and implementation PF related TFS, including mechanism of communicating UNSCRs to OEs in a timely manner.

c) Bulgaria should ensure that all supervisors receive appropriate training, have powers, and adequately supervise and monitor PF-related TFS, and not limit it only to sanction screening tools.

d) Bulgaria should provide guidance to OEs specifically on the implementation of the PF-related TFS and respective mitigating measures.

369. The relevant IOs considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

4.2. Immediate Outcome 9 (TF investigation and prosecution)

370. The criminalisation of TF has been improved since the adoption of the previous MER to comply to a greater extent with the standards, including the coverage of all "*treaty offences*" and provisions on foreign terrorist fighters. As result, the TF offence is now broadly in line with the standards and the remaining technical deficiencies described under R.5 of the TC Annex do not seem to prevent the Bulgarian authorities from identifying and pursuing any criminal activity related to TF.

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

371. As discussed under IO.1, the NRA adopted in 2019 identified a number of high-level TF risk events in Bulgaria, such as the widespread use of cash and MVTS, with occasional use of illegal value transfers (*hawala*) as derivatives of the large cash-based and informal economy. The authorities consider that these are the main vehicles for transferring funds related to TF particularly by migrant communities. The potential diversion of funds allocated by NPOs for charitable or religious activities in Bulgaria towards TF was noted as another TF-related risk.

372. Bulgaria has no TF prosecutions or convictions so far. Both TF cases that have ever been instituted are still being investigated in pre-trial proceedings. While one of these TF cases is still at an early stage of investigation, the other one (see case box 3.11 below) has sufficiently been explored to demonstrate that most of the TF-related risk events mentioned above might occur in practice and that Bulgarian authorities have been, at least in this case, capable of prosecuting more sophisticated types of TF activities such as the provision of non-monetary support to terrorist organisations.

Box: 3.11: TF directed outside the country

Six persons (out of whom 5 were Bulgarian and Syrian dual citizens) have been charged by the SPO with TF crimes (under Art. 108a, para 2 of the Penal Code, etc. under Art. 109, para 3, item 2, in conjunction with para2 of the Penal Code).

The defendants were directed outside from Bulgaria and transferred the funds through the "*hawala*" system to persons in Turkey, from where the funds were sent to Syria, in order to purchase high–tech equipment to be used for terrorist acts. As a result, off–road vehicles (jeeps, pickups) were purchased in other European countries (Germany, Romania), which were transported from Bulgaria through Turkey to Syria to local terrorist organizations as well as to other armed opposition groups. Individuals had personal codes that they exchanged with each other to identify themselves, and the money was handed over "*by hand*". It is unknown whether the vehicles were later used in practice in terrorist crimes.

Different investigative techniques were used: numerous witnesses were interrogated, including interrogations before a judge, as well as interrogations of witnesses with secret identities; some of the accused gave explanations; identifications were made; written evidence was collected (letters from mobile operators; protocols for inspection of material evidence; Bulgarian Personal Documents reports, printouts from the Commercial Register, reports on trips abroad) and physical/material evidence, and material evidence were analysed (SIM). In addition, forensic computer–technical and economic expertise and ballistic and fingerprint examinations have been conducted.

As it was explained by the authorities, the financial profile of the perpetrators was subject of meticulous examination which confirmed that they had not used any legitimate means for financial transactions and thus the involvement of the FI/DNFBP sector could be excluded. This led authorities to examining the transfer of funds through the "*hawala*" system. As a result of this, eight European Investigation Orders were issued to confirm information about individuals operating the "*hawala*" system outside Bulgaria.

373. The case above, although representing the one and only successful TF pre-trial investigation so far in Bulgaria ("*successful*" in terms of evidential results and accusations) undoubtedly demonstrates an ability to effectively investigate complex TF cases in line with the country's TF risk profile. In this case, it included the consideration of the geographical and geopolitical position of Bulgaria with transnational links to neighbouring countries and eventually to the conflict zones, the involvement of migrant communities and, first and foremost, the successful demonstration of capability of Bulgarian authorities to identify and investigate transfers of funds made through complex and illegal methods (*hawala*).

374. Notwithstanding that, this is just one single TF case, which cannot serve as a basis for drawing general conclusions and which cannot in itself confirm and validate all findings of the NRA. While the law enforcement and prosecutorial authorities demonstrated an outstanding performance in this very case, the same approach was regrettably missing in other cases where, as discussed below, potential TF aspects of terrorism-related cases were not examined, which implies a limited and uneven understanding of TF-related risks by the same authorities.

375. As noted under IO.1, the TF risk assessment and risk understanding in Bulgaria was obstructed by a lack of data relating to financial flows and FIs/DNFBPs. Therefore, the exposure of the financial and non-financial system in Bulgaria to TF is not in all cases well understood and/or known (even if no such channels appear to have been used in the case described above). Bulgaria has not adequately considered the TF risks associated with the vulnerabilities in its financial system or its broader AML/CFT regime and has not conducted adequate analyses in relation to specific financial products or non-financial services known to be vulnerable to terrorist exploitation such as cross-border cash movements.

376. In addition, and apart from the one TF case mentioned above, the AT consider that Bulgaria currently only has a developing understanding of how the geographical position of Bulgaria and the trafficking of cash through the Balkan route manifests as a TF risk in the country.

377. As for the terrorism-related risks discussed in the updated National Security Strategy (2018), it appears that the most concrete types of threat Bulgaria faces are, from an external perspective, the increasing presence of religiously motivated groups in the region with favourable environment for the dissemination of their radical ideologies, establishing logistical bases and recruiting foreign terrorist fighters, and from an internal perspective, the extreme poverty, social exclusion and marginalization of some communities that makes them vulnerable to radical religious and other extremist ideologies. Migration was mentioned as another threat, considering the geographical position of Bulgaria that predetermines a constant flow of illegal migrants with a potential for foreign fighters passing through the country and for the formation of terrorist and logistical cells in Bulgarian territory.

378. Although the AT was not provided with adequate statistics, the case examples presented by the authorities showed that in the assessed period, there were at least 4 confirmed cases of individuals traveling to conflict zones (e.g., Syria). Most of these cases indicated a simple *modus operandi*, with only the aspiring foreign fighters having been captured while crossing the border, and the investigation was not extended to any external recruiters, organisers, or financiers. Bulgarian law enforcement and prosecutorial authorities have not investigated the financing dimensions of these cases, which must have happened due to the presumption that the perpetrators travelled on their own and financed their travel costs for themselves. It was not demonstrated to the AT that in the provided cases these aspects had been considered and examined to any extent by the authorities, despite certain factors in concrete cases that might

have given rise to the suspicion that the travel of the individuals had actually been organised - and possibly also financed - by others. Disregarding the associated TF aspects might be attributed to the limited and uneven understanding of TF risks by the Bulgarian pre-trial authorities responsible for the investigation and prosecution of the respective criminal cases.

379. As for the other TF-related threats, the involvement of the NPO sector was not represented to any extent in the case examples presented to the AT. There has been no case where the suspicion of TF was related to NPOs serving as hubs to channel money from or into Bulgaria for any terrorism-related purposes (even for disseminating religious fundamentalism). The authorities however advised that they had identified the possibility for such an abuse, but no such TF-related threat had been materialised.

380. Migration and migrant communities, as another TF/CT threat, could be noted in the case studies considering that a significant proportion of the terrorism-related cases (and also the TF case described above) had been committed by people of foreign (Middle Eastern or Maghrebi) origin. Nonetheless, there was no case presented to AT to demonstrate the actual relevance of the recently increased migrant flow in relation to terrorist activities (including the recruitment and travel of foreign fighters) and related TF. The AT was provided no information as to whether and to what extent these threats have manifested in concrete cases with the suspicion of terrorism or TF (in either pre-investigative or pre-trial phase) and if not, whether such threats have successfully been disrupted by any other administrative means.

381. Beyond these cases, Bulgaria observes that no terrorist groups or recruitment networks have been discovered on its territory in the period under review. Also there has only been a single terrorist act committed on Bulgarian soil ever, the terrorist attack on the Sarafovo Airport (Burgas) in July 2012, years before the assessed period (the other TF case that is being investigated at the moment is related to the financial aspects of this particular terrorist offence).

4.2.2. TF identification and investigation

382. In the pre-investigative stage of proceedings, criminal information on TF and terrorism-related activities is gathered and analysed primarily by the Counter-Terrorism Department of SANS (CTD-SANS) and, in some cases, by the Counter-Terrorism Department of the GD-COC. The operational activities of the CTD-SANS involve a wide spectrum of various measures from human sources to SIMs and international cooperation, with an output the quality of which was praised by all other competent authorities.

383. The CTD-SANS has a wide competence in the CT/CFT field, including the detection, prevention and disruption of attempts for terrorism and TF, operational control and counteraction against extremist (religious or other radical) organizations, and analysis and terrorist threat assessment. Both TF-related pre-trial investigations were initiated upon information collected by the CTD-SANS and reported to the SPO. On the other hand, the CTD-SANS deals with a remarkable number of terrorism (and TF) related operations (75 in 2020 and 14 in the first 9 months of 2021) only a fragment of which results in referrals to the prosecutor, but this can be explained by the specific characteristics of these criminal activities.

384. Pre-trial investigations of terrorism-related criminal offences (including TF) fall under the exclusive competence of the SPO. Investigations are thus carried out by an investigator from the Investigation Department of the SPO and supervised by a prosecutor from the SPO. Furthermore, terrorism-related cases are, in both bodies, handled by specialists: investigators

from a special CT section of the Investigative Department of the SPO, and prosecutors from a similar, separate department of the SPO specifically dealing with terrorism-related criminal cases (the head of which department is one of the deputy administrative heads of the SPO). Once an indictment will have been issued in a TF case, it will be tried by the Specialized Criminal Court.

385. As opposed to the criminal investigation of ML offences, where one can find quite a few investigating and prosecuting bodies with equal competences but different levels of experience and expertise (see IO.7) the roles and responsibilities are incomparably clearer in the field of TF investigations. The separation of the investigative and prosecutorial departments as described above allows the work on terrorism-related cases to be carried out by specialists who have gained experience in this field, while the same structure also provides for the prioritization of those cases. For the moment, the current structure appears to be adequate, and the authorities involved seem to be satisfied with their human and other resources available. However, this arrangement can only be maintained until the number of terrorism-related and TF cases remains at the present (very low) level while any significant increase would have immediate negative impact on capability to investigate and prosecute TF cases effectively.

386. In the 2 TF cases currently pending in the pre-trial stage, the authorities reported of a close and effective cooperation between the respective prosecutors and investigators, as well as with the CTD-SANS the experts of which provide, upon a formal request, operational (analytical and other) support to the prosecutor or the investigator so as to achieve and maintain a targeted, intelligence-based approach. In this respect, the same goes for the FID-SANS which, upon the request of the CTD-SANS, provided information on checks of 205 persons in relation to Case described above related to the export of vehicles to Syria as well as on 2 currency exchange offices and 1 accounting firm.

387. Notwithstanding this, the low number of TF-related criminal cases does not provide a sufficient basis for drawing conclusions as to the availability, use, and usability of financial intelligence for the purposes of TF investigations. It appears, that no input from the FID-SANS has had much, if any, relevance in initiating criminal proceedings for TF or terrorism-related offences in Bulgaria. As it was repeatedly confirmed by prosecutorial authorities, no pre-trial investigations for such offences have ever been based, directly or indirectly, on any initial dissemination by the FID-SANS, which must primarily be attributable to the generally low quality of TF-related disseminations. As discussed more in details under IO.6, the FID-SANS, when dealing with TF-related STRs, tends to sacrifice quality on the altar of urgency, disseminating all available financial information immediately but without having performed an in-depth analysis, which seriously limits the value and quality of the output.

388. In addition, the quality of the FID-SANS products is also caused by the similarly low quality of TF-related STRs originating from the low understanding of TF-related risks by the reporting entities. The AT learnt that TF-related STRs were in most cases made upon partial matches with UN sanction lists (which all turned out to be false-positive) and the respective transactions and funds being linked, to any extent, to countries with high risk for TF or terrorism (which practically meant reporting any Middle Eastern or Maghrebi links that occurred). For the period 2014-2020 the FID-SANS received 207 TF-related STRs, the information from which was disseminated to the CTD-SANS. Further analysis performed by the CTD-SANS did not confirm the TF suspicion in any of these referrals (only 13 disseminations were eventually forwarded to LEAs for investigating other offences).

389. Apart from CT operational information and the FID-SANS disseminations discussed above, the Bulgarian authorities also mentioned a range of other sources they may use in order to identify potential TF cases, such as the results from parallel financial investigations, information from other national competent authorities and information from other jurisdictions or international bodies. No pre-trial investigation of TF has so far been initiated upon information coming from such sources, although the effective exchange of TF-related information among the competent authorities in Bulgaria and with foreign counterpart authorities was demonstrated for the investigation in both TF-related pre-trial investigations.

390. As far as concrete cases are concerned, as noted above, the identification of TF activities and the reporting of the case to the SPO was in both occasions carried out by the CTD-SANS. In the first case, as described above, the TF acts have been committed in an organised manner with significant complexity and international implications, and the fact that TF charges have already been pressed against multiple individuals generally appears to demonstrate the applicability of the legal framework and the ability of Bulgarian authorities to successfully identify and prosecute large-scale TF schemes.

391. Whether or not the performance demonstrated in this case was just an exception to the rule can better be illustrated by the second, more recent TF case. As noted above, this is related to the single major terrorist act in Bulgaria (2012) the perpetrators of which were finally convicted and sentenced in September 2020. For reasons that remained unknown to the assessors, however, the related TF activities were not subject of investigation until October 2020, that is, not before the conviction of the terrorists responsible for the terrorist act itself. No authorities met onsite made reference to any hypothetical requirement to await a prior conviction for the terrorist act so that the related TF activities can be investigated, but the sequence of events appears to imply something more than a coincidence. In any case, the AT has some concerns that such an eight-year delay may hinder any effective investigation of the TF activities (particularly as these appear to have been committed, at least partly, from abroad).

392. Identification of TF would appear more likely to occur while investigating the terrorism-related activities. As noted above, however, the investigation of the financial aspects of the relatively few cases related to terrorism (mainly consisting of the travels of foreign fighters) appears not to take place as a policy and indeed, the AT were not provided with any information or evidence to demonstrate that TF is examined in all terrorism-related cases. The presented terrorism-related case examples suggest that the authorities likely presumed, in lack of any contradicting *prima facie* evidence, that the aspiring foreign fighters, who attempted to travel to conflict zones for pursuing terrorist purposes, had financed their respective costs for themselves. It was not clear, however, whether and to what extent the role of recruiters and organizers was subject of examination (or any persons who gave them instructions as to when and where to go and by what means) that could have revealed any associated acts of financing.

393. This aspect was particularly missing, for example, in a case[46] where the perpetrator travelled five times to Syria (and back) for pursuing terrorist purposes in a two-year period before being apprehended. This must have required a stable financial background and might easily have involved external financial input as well, which had most likely originated from the precisely identified terrorist organisations the individual reportedly contacted and joined in

[46] SPO file No. 148/2020.

Syria. In another case[47], the foreign fighter returned from Syria to Bulgaria to improve his shooting skills and spent months in professional shooting clubs receiving intensive training, which also must have required finances the source of which does not seem to have been properly assessed.

394. As far as the two TF investigations are concerned, the authorities have not imposed any measures to secure terrorism-related funds or equivalent value. While this is to some extent understandable in the TF case related to the Sarafovo Airport incident, it is far less evident in the other case described above. Considering the significant amount of funds involved which will eventually be subject of confiscation, one would expect some provisional/precautionary measures imposed to secure these confiscation measures. In addition, the authorities confirmed that no bank secrecy was disclosed, and no bank accounts blocked in the same case (which could have taken place in the context of a parallel financial investigation even if the perpetration of the TF offence only involved illegal value transfer services).

4.2.3. TF investigation integrated with –and supportive of- national strategies

395. In the assessed period, Bulgaria has adopted a number of national strategies with more or less AML/CFT elements, out of which only the National Security Strategy (for 2011-2020) and its updated version (for 2018-2025) cover, to some extent, CT and CFT issues. The updated National Security Strategy is the only one that actually contains CFT elements, requiring that the security services, public order services and the armed forces counter the global threat of terrorism in a unified and coordinated manner to prevent, intercept and to prosecute attempts, among others, to build structures of terrorist and extremist organizations in Bulgarian territory and to provide logistical support, including raising funds, for the benefit of international terrorist and extremist organizations. The rather generic character of this strategic document, however, prevented the AT from establishing whether and to what extent it had been based on conclusions drawn from TF investigations.

396. The NRA contains a separate (and restricted) chapter dedicated to TF risks. This analysis was to a large extent supported by information on trends and typologies gained from experience in investigations of TF or terrorism-related offences, with detailed description of the respective criminal cases. After the adoption of the NRA, however, the necessary steps to mitigate TF risks did not materialize in a formal strategy or action plan until mid-September 2021, the adoption of the Action Plan for addressing ML/TF risks established in the NRA. In this Action Plan, the actions reported to have taken place from 2019 to 2021 were mostly ML-related while those related to TF apparently have not been based on supporting information gained from TF investigations (e.g., on any legal or institutional vulnerabilities) and the same goes for the actions planned for the forthcoming period.

397. As discussed more in details under IO.10, the LMFT provides for a mechanism for designating natural persons as individual terrorists on a domestic list pursuant to UNSCR 1373 (see Art. 5 LMFT). The range of persons to be listed includes those against whom criminal proceedings have been instituted for practically any criminal offences related to terrorism (including the TF offence), as well as those for whom there is sufficient data that they engage in activities related to terrorism or TF. A consolidated list which includes, among others, individuals

[47] SPO file No. 413/2016.

falling in these categories (listed under Section III and Section IV, respectively) was issued in 2003 by Decision № 265 of the Council of Ministers and has since been amended four times, last in 2016. The individuals designated domestically are thus listed in Sections III and IV of the consolidated list, where one can currently find 4 names in Section III and 2 in Section IV. This fact demonstrates that Bulgarian authorities had actually used the results coming from terrorism-related investigations to support domestic designations of terrorists and financiers of terrorism.

398. On the other hand, the implementation of this mechanism suffers from some serious flaws. The number of designated persons listed in Sections III and IV has not been updated since 2016 and is therefore obsolete, not reflecting the numerous accusations for terrorism-related offences that have since taken place (only in the case examples provided to the AT, one can find 18 persons having been accused of terrorism-related criminal offences since 2016 out of which 6 of TF). Results of the investigations related to terrorism or TF (including the remarkable number of terrorism-related accusations) thus were not used for domestic designations in the greatest part of the period under review – and neither were used for making any proposal to include the same individuals in the corresponding UNSC list. As a consequence, the results of the investigations related to terrorism or TF are not adequately used to support national CFT strategies in this respect.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

399. There have been neither convictions nor indictments for the TF offence (Art. 108a [2] CC) in Bulgaria and therefore no sanctions or measures have been applied for TF the effectiveness, proportionality, and dissuasiveness of which could be assessed.

400. As described in the TC Annex, however, the range of punishment available for TF has been lowered in the CC (to a maximum sentence of 12 years instead of 15 years) and the possibility for applying additional fines has been eliminated, which reduced the proportionality of the sanctions.

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

401. The AT have no information on any other criminal justice measures to disrupt TF activities where it is not practicable to secure a TF conviction for a natural person, considering that the TF offence in Art. 108a (2) CC, as amended, is broad enough to cover practically all potential TF activities related to any sorts of terrorism-related offences in the CC. As a result, conducts that cannot be subsumed under Art. 108b (2) are highly unlikely to occur in practice. The AT was assured by the authorities that no pre–trial proceedings for TF have so far been terminated without an indictment and neither have there been cases of refusal to initiate pre–trial proceedings for TF.

402. As discussed in C.3.10 of the TCA, no criminal conviction for a corporate entity is possible in the Bulgarian law but a "quasi-criminal" administrative liability applies. Pursuant to the Administrative Violations and Sanctions Act, a financial penalty can be imposed on a legal person having enriched itself from a proceeds-generating crime (including TF) or having committed any crime upon order of an OCG, when that crime was committed by a responsible person of the same legal entity. These preconditions are however too specific to make this administrative liability effectively applicable in TF cases against legal entities and indeed, there have not been such cases in practice.

403. The authorities also reported the possibility of recourse to other administrative measures against natural persons such as deprivation of nationality, deprivation of residence status, denial for provision or deprivation of asylum right, ban on entering and residing in Bulgaria and in the Schengen area and expulsion to the country of origin or to a third country. The AT learnt that some or more of these measures are imposed with regularity on individuals allegedly related to terrorism, where data are insufficient for criminal proceedings (no exact figures in this respect were available). Regarding legal persons (including NPOs) the Law for Counteraction to Terrorism provides for the dissolution of a legal entity that can reasonably be presumed to have been associated with the preparation, aiding or perpetration of terrorism (including TF) although the AT were not informed of any concrete cases where such administrative measures had been imposed during the evaluation period.

Overall conclusions on IO.9

404. Bulgaria has improved its TF criminalisation which now complies to a greater extent with the standards, as result of which the TF offence is now broadly in line with the respective standards.

405. The perception and understanding of TF related risks by the competent authorities is generally uneven and limited (with occasional exceptions such as in the one successful TF case so far) that fails to adequately address all characteristics of potential TF activities in Bulgaria and the region. Generally low understanding of the TF risks by FIs and DNFBPs results in low-quality STRs which generate low-quality FIU disseminations in relation to TF.

406. Bulgaria does not have a national CT or CFT specific strategy and it was not demonstrated that TF investigations were integrated with or supported CT/CFT-related other strategies. Outcomes of terrorism-related criminal proceedings are not adequately used for designations of terrorists or terrorist organisations.

407. The investigating and prosecuting authorities generally demonstrated the sufficient specialisation, experience, and cooperation in, and proper prioritization of terrorism-related or TF cases.

408. While a limited number of terrorism-related offences have been prosecuted or even resulted in convictions, there have been no prosecutions and convictions for TF in Bulgaria with only 2 cases pending in pre-trial proceedings. Although one of the latter demonstrated the authorities' capability of prosecuting complex TF structures, the authorities did not generally demonstrate having an effective and systematic approach to explore and investigate the financing aspects of the terrorism-related offences

409. **Bulgaria is rated as having a moderate level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for TF without delay

410. Bulgaria implements TFS in relation to terrorism financing (TF) through EU Regulations supplemented by the national legislation -the Law on Measures against the Financing of Terrorism (LMFT). The national mechanism provided in LMFT supplements the EU framework and overcomes the delays of transposing UNSC designations into the EU framework (see assessment team's analysis in R.6).

411. The Ministry of Foreign Affairs (MFA) is the central authority vested with powers of transposing UNSCRs through publishing them on its website, after which they become part of national legislation and thus are binding for all natural and legal entities. The website of MFA contains a direct link to UN consolidated sanctions list which is automatically updated by relevant UN Committees upon any changes. This ensures that any changes in the UN sanction lists are automatically effective in Bulgaria once the relevant UN Committees update their own website. Therefore, funds and other assets owned or controlled by the designated persons and entities are to be frozen immediately as envisaged by the LMFT.

412. Besides, the MFA also sends notifications on newly adopted or amended UNSCRs to all relevant state authorities, including but not limited to the FID-SANS, BNB, FSC and etc. either via automatic exchange system or by physical letters. According to the MFA, the notification is sent as soon as the relevant UNSCR is received from the permanent mission of Bulgaria in the UN. The process may take up to 2 days and authorities explained that the delay in notifications is caused mainly by the 7 hours difference in time zones between Bulgaria and the USA. Competent authorities, except for the FID SANS, rely on the notifications sent by MFA, to update the links to UNSCRs on their websites or to send the information to the entities supervised by them. Except for the BNB, other competent authorities do not notify the private sector on newly adopted UNSCRs, as well as amendments made to them, and only publish the link to the UNSCRs on their websites. As regards the BNB, the latter sends notifications to financial institutions usually within a week from getting information from the MFA. Therefore, while the Bulgarian legal framework and practical measures taken by the MFA transpose the UNSCRs within hours, the process of communication, is not done in a constant and timely manner, which could hinder the effective implementation of UNSCRs.

413. Bulgaria has not proposed or made any designations pursuant to UNSCR 1267. At the same time, the authorities were aware and could elaborate on the mechanisms, evidential thresholds as well as designation criteria to be applied, mainly referring to those in the respective UNSCR with main authorities involved in the processes being the SANS and MFA.

414. Bulgaria has demonstrated a practical implementation of the UNSCR 1373. Particularly, the national list was adopted on 18.07.2003 with Decision № 265 of the Council of Ministers and since then several changes have been introduced, the last one in August, 2016. The Council of Ministers` decisions are promulgated in the State Gazette and published on the websites of the SANS and MFA. There are currently six persons on the national list, out of which two were listed on the grounds of the availability of sufficient data for terrorism (no pre-trial proceedings at the time of designation), while the other four in the view of initiated pre-trial proceedings for terrorism. On the other hand, as mentioned under IO.9, the implementation of this mechanism suffers from some serious flaws. The number of designated persons listed in Sections III and IV has not been updated since 2016 and is therefore obsolete, not reflecting the numerous accusations for terrorism-related offences that have since taken place (only in the case examples provided to the AT, one can find 18 persons having been accused of terrorism-related criminal offences since 2016 out of which 6 of TF). The results of recent investigations related to terrorism or TF (including the remarkable number of terrorism-related accusations) were not used for domestic designations in the greatest part of the period under review – and neither were used for making any proposal to include the same individuals in the corresponding UNSC list. No foreign jurisdiction has ever requested application of restrictive measures by the Bulgarian authorities. At the same time, the competent authorities demonstrated awareness on the procedures to give effect to such requests. No funds have been frozen with regard to TFS in relation to TF.

415. There are no mechanisms and publicly known procedures in place for delisting individuals or entities and unfreezing of assets with regard to UNSCRs 1276 and 1988. During the interviews the authorities provided contradicting answers with regard to the competent authority to whom such requests should be addressed. The mechanism for delisting and unfreezing with regard to UNSCR 1373 is envisaged in the LMFT.

416. All OEs, including VASPs, showed at least a basic awareness of their obligations in relation to TF TFS, but FIs, especially banks (the most important sector in terms of materiality), demonstrated good understanding. OEs, with some exceptions, mentioned that in case of a full match they would immediately freeze the fund, suspend the provision of services and inform competent authorities as envisaged by LMFT. Compared to the FIs, the DNFBPs and VASPs had less developed level of understanding and implementation of TFS related obligations. For more information in relation to understanding, awareness and application of TF TFS obligation by OEs as well as relevant shortcomings identified by the AT please refer to IO.4.

4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations

417. Bulgaria identifies all associations and foundations operating in the country as falling under the FATF definition by virtue of their legal formation. The sector is quite big in terms of materiality and consists of 40 627 associations and 8 173 foundations, all of which are considered as falling under the FATF definition. As for the subset of NPOs being at risk for TF, the Bulgarian NRA contains some analysis on the NPOs within the TF risk assessment part. This analysis identifies religious organizations operating internationally as being more vulnerable to TF abuse. No statistics available on the number of such entities. The NRA further rates the risk of TF abuse of the overall NPO sector as medium. According to authorities, the NPOs are not considered as a source of TF in Bulgaria. It should be noted that, some part of the data used was from NPO sectorial assessment done in 2012, however, as stated by the authorities the information collected for the overall TF risk assessment was also used. From the interviews the AT was informed that the representatives of the NPO sector itself was not involved in the process of data collection for the purposes of the NRA, except for the provision of some statistical data by the BCNL.

418. Based on the information provided to the AT the activities and vulnerabilities of NPOs were not analysed, including donors, founders of NPOs, donations and main directions of disbursements, any connections with high risk or conflict zones, transactional data and etc. In addition, the extent of the use of data from NPO sectorial assessment done in 2012 is not clear, thus raising major concerns on the relevance of thereof. Overall, the impression of AT is that the limited analysis of NPOs within the 2019 NRA TF risk assessment part is not comprehensive and substantiated with relevant case examples or other information. The AT and authorities share the view that there is a need for further comprehensive analysis of the NPOs to determine the extent of their TF abuse. At the time of the onsite the NPO sectorial risk assessment was in process of being conducted and would be finalized in the next update of the NRA.

419. All NPOs operating in the country have to register and are obliged to publish annual reports, including financial statements. The National Revenue Agency is the controlling body empowered to impose sanctions when the obligation for publishing the reports is not followed by the entities. In addition, there are stricter requirements for NPOs operating for the public benefit. These NPOs need to prepare annual activity reports and financial statements, which need to be published and entered in the register each year. Data related to donors, and the use of

resources shall be provided in the report. The Registry Agency has the right to suspend the public benefit status of any NPO which has not published its annual reports for two consequent years. This was not tested in practise due to the prolonged deadline for compliance with new requirements. It should however be noted that the substance of reports is not checked neither by the Registry Agency, nor by the National Revenue Agency. By virtue of the LMML the information in relation to donors and related information should be checked by the FID-SANS which is vested with powers to supervise NPOs as OEs.

Supervision of the NPO sector

420. All types of NPOs are OEs with limited obligations according to the LMML and are supervised by the FID-SANS. The supervision of the sector is based neither on the results of NRA nor on other TF related risk assessment. Since 2018, neither supervision nor monitoring was conducted towards the sector, and before that, the numbers and content of supervisory activities were not targeted at high risk NPOs. Other competent authorities, such as law enforcement agencies, also do not proactively monitor the sector for identifying any patterns or risks of TF abuse and stated that they would mainly reach out to the specific NPOs in case of a TFS hit, an STR or in case of information from other countries.

421. Although not tasked with supervising NPOs, the National Revenue Agency together with the Registry Agency conducts monitoring towards the submission of financial statements by associations and foundations. According to the established organization of work, after the deadline for submission of annual financial statements, the Registry Agency submits information to the National Revenue Agency on all persons who have not fulfilled their obligation to submit annual financial statements. The Revenue Authority initiates actions to impose administrative penal liability in all cases. Respectively, in 2020, 161 administrative penal proceedings were initiated against NPOs.

Outreach to the NPO sector

422. A number of outreach and educational activities have been provided to the NPO sector, however with limited focus on their sectoral risk of TF abuse. This included adoption of model internal rules and methodology for risk assessment for NPOs. An important workshop dedicated to protecting the Bulgarian NPOs from TF abuse was organized in 2021 by the Centre for Financial Crime and Security Studies at RUSI in collaboration with FID-SANS. Some of the NPOs mentioned that the guidance and outreach provided by the FID-SANS together with sector representatives in relation to the risk of TF abuse had an increasing tendency during recent years. No dedicated outreach was provided to the donor community, except for the one conducted in 2021. Together with existing legislative requirements concerning the limitation of the use of cash, some outreach activities, such as round table discussions involving representatives of banks and NPOs were conducted by the support of authorities to encourage the NPOs to use regulated financial channels. This has resulted in increased use of regulated channels by the NPO sector.

423. A positive tendency should be noted that, the representative of the NPO sector interviewed during the on-site visit were aware to some extent of their TF risks and applied mitigation measures, which also include identification of donors and beneficiaries. Most of the NPOs met onsite did not receive any outreach or training from the authorities, however applied mitigating measures due to the rules and procedures in place by parent NPOs or major donors. All representatives of the sector highlighted the importance of an in deep sectorial TF risk assessment, identification of NPOs at risk and revision of existing obligations based on the existing risks.

4.3.3. Deprivation of TF assets and instrumentalities

424. No assets have been frozen pursuant to the sanctions regime under UNSCR 1267/1989 and 1988. It is the opinion of both the Bulgarian authorities and the OEs, met on-site, that if funds or other assets are identified, these would immediately be frozen. As a matter of practice, FIs would not proceed the transaction until convinced that all parties in the transaction are not in the UN sanctions list. FIs and DNFBPs confirmed that upon a freezing action taken under the TF-related TFS regime, and even in case of false positives, they would immediately report to the SANS, FID-SANS, MOI. Banks, postal service providers and e-money institutions had cases of potential matches and that they notified to competent authorities to be certain that they were false positives. Particularly, there were 4 STRs concerning partial matches with sanctions lists, out of which 1 was related to a partial match with UNSCRs. The matches mostly concerned subjects holding the same or a similar (nick) name as the designated person. The FID-SANS indicated that all reports were analysed with priority, and even in the case of a "false positive" all cases were still later disseminated to the STD-SANS in a timely manner. The STD-SANS conducted additional detailed analysis and confirmed cases to be a "false positive" match.

Box 4.1: **Partial match with UNSCRs and cooperation between the FID-SANS and the Counter-Terrorism Specialized Directorate of the SANS**

The case concerns a partial match in UN lists on a client of Bulgarian bank (born in African country with passport from European country). The match was based on combination of names and citizenship, however not a full match with date of birth (or other identifiers). Besides, there were suspicious transactions with funds with unknown origin. Those include incoming transfers received from payment institution in European country followed by cash withdrawals and debit card payments in Bulgaria. FID-SANS provided the results of its analysis to competent directorates within the SANS (Counter-Terrorism Specialized Directorate and Financial Security Specialized Directorate). The Counter-Terrorism Specialized Directorate of the SANS performed operative checks and used its operative sources to establish that the subject is a student in Bulgaria and received funds from her parents for the student expenses. Additional data was acquired on the address and the family relations of the subject in the foreign country. The additional checks completely discarded a full match on the subject with sanctions lists.

425. There are two ongoing investigations on TF offences (both in pre-trial stage), however no terrorism-related funds were restrained in the mentioned cases. As indicated under IO 9, the investigation of the financial aspects of the relatively few cases related to terrorism appears not to take place as a policy, which hampers also the effectiveness of deprivation of TF related assets and instrumentalities by LEAs.

426. Bulgaria does not have experience in fully or partially unfreezing funds as no assets have been frozen pursuant to the UN TFS regimes. As mentioned earlier, no precise mechanisms and publicly known procedures are in place for delisting and unfreezing with regard to UNSCRs 1276 and 1988, and there is a lack of understanding on the mechanisms and competent authorities available in case of such requests.

4.3.4. Consistency of measures with overall TF risk profile

427. The NRA identifies the high-risk TF risk events in Bulgaria as follows: (i) use of MVTS and informal value transfer (hawala) to transfer funds potentially related to TF; and (ii) facilitation by migrant communities aggravated by large cash-based and informal economy. The NRA also notes that the potential diversion of funds allocated for NPO or religious activities in Bulgaria

towards TF is of medium risk. However, there are some doubts as to the comprehensiveness of understanding of TF risks (see also IO.1). As mentioned in the IO.1, the analysis of TF risks is limited to a basic understanding of the cash economy in Bulgaria and only a limited appreciation of geographical factors influencing TF risk. Besides, the activities and vulnerabilities of NPOs were not analysed, including donors, founders of NPOs, donations and main directions of disbursements, any connections with high risk or conflict zones, transactional data and other. These factors significantly hamper the understanding of TF risks by the authorities, thus the effectiveness and consistency of the measures applied is under doubt.

Overall conclusions on IO.10

428. Bulgaria has a mechanism in place, which enables to overcome the delays between the designation decision taken by the UNSCs and its transposition into the EU framework. At the same time there are major concerns that the process of communicating new designations and amendments to the lists are not done in a constant and timely manner. Bulgaria has demonstrated a practical implementation of the UNSCR 1373. On the other hand, as mentioned under IO.9, the implementation of this mechanism suffers from some serious flaws. The results of recent investigations related to terrorism or TF (including the remarkable number of terrorism-related accusations) were not used for domestic designations in the greatest part of the period under review – and neither were used for making any proposal to include the same individuals in the corresponding UNSC list

429. All OEs showed at least a basic awareness of their obligations in relation to TF TFS. At the same time deficiencies identified under IO 4 in relation to implementation of TFS related obligations negatively impact the overall effectiveness of TFS regime. TF risks emanating from NPOs have not been comprehensively assessed in the NRA. Accordingly, no focused, proportionate measures are applied towards this quite material sector nor is it adequately supervised or monitored. There are doubts remaining in relation to TF risk understanding and consistency of measures applied by Bulgarian authorities. Given the risk and context of Bulgaria (e.g. geographical location, existence of terrorism related cases, limited understanding of TF risks, large cash-based grey economy and etc.) the above mentioned findings are considered to be fundamental.

430. **Bulgaria is rated as having a moderate level of effectiveness for IO.10**.

4.4. Immediate Outcome 11 (PF financial sanctions)

431. In terms of underlying proliferation and proliferation financing risks, there are several contextual factors that are duly acknowledged by the Bulgarian authorities, including well-developed industry for manufacturing and trading with defence related and dual use goods, presence of technology and knowledge, which may be of interest to end users of concern, as well as geographical location that could be exploited for smuggling of goods, potentially proliferation sensitive. At the same time, Bulgaria is not a financial centre and the risks of complex schemes for evasion of sanctions are not particularly relevant. Bulgaria has introduced a robust export control regime with multi-layer defence to mitigate the risks in relation to proliferation through the central coordinating body being the Inter-ministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction. The activities although indirectly also included some financial aspects, including checks with UNSCRs related to PF and ad hoc information sharing with FID-SANS.

432. Bulgaria holds diplomatic and trade relations both with DPRK and Iran. There is an Embassy of DPRK in Bulgaria, which as confirmed by the authorities is being closely monitored. Particularly, in 2017 competent directorates within SANS (incl. FID-SANS) explored the availability of bank accounts in Bulgaria and the financial operations of the Embassy of DPRK in Bulgaria by obtaining information from all banks in Bulgaria. The findings were shared with the Panel of Experts of the UNSC Committee of Resolution 1718 through the MFA. In the last years, bilateral trade volume was very low and consisted of Bulgarian exports to DPRK (2015: USD 1.0 mln.; 2016: USD 0,6 mln; 2017: USD 0.6 mln.; 2018 and 2019: USD 0.0; 2020: USD 0.7 mln. (mainly export of food products for 680 thousand USD); January - October 2021: USD 0.0).

433. As for Iran, there is an Iranian embassy in Bulgaria. The trade relations with Iran in 2020 amounted to approx. 0.34% of exports and 0.06% of imports of Bulgaria. In 2020 Bulgaria's The majority of exports to Iran are agricultural products (particularly maize, which accounted to app. 53.4% of overall export). Other export items are machinery and construction materials. In 2020 Bulgaria imported from Iran products of the chemical industry (polymers of ethylene and polymers of styrene, both of which accounted to app. 66% of overall import) and ferro-alloys, fresh and dried fruits, float glass and surface ground glass.

434. The Inter-ministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction has not granted any licenses nor received any requests for import and export of defence-related products and dual-use items for Iran and DPRK.

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

435. Bulgaria implements TFS related to PF through EU regulations and thus is generally impacted by the delays between the designation decision taken by the UNSCs and its transposition into the EU framework. The EU mechanisms do not have technical problems in relation to the time of their transposition when it concerns Iran. Individuals and entities had already been listed by the EU when their designation by the UN was made. As for the TFS against DPRK, incorporation into the EU legal framework of the most recent additions made to the UN list of designated persons and entities (of 02 June 2017, 05 August 2017, 11 September 2017 and 22 December 2017) took 8 days, 6 days, 5 days, 4 days and 17 days respectively. Hence, despite recent improvements, delays in implementation of the UNSCRs of DPRK still occur. The authorities mentioned that the general legal framework (in particular, the Constitution, the Act on International Agreements) gives the ability to the Council of Ministers to overcome the delay and transpose the UNSCRs directly, however, the mentioned legal provisions were not tested in practice during the assessed period.

436. As mentioned earlier, due to the reliance on EU regulations, there is no dedicated authority or committee responsible for implementation of UN TFS in relation to PF. At the same time, since all UNSCRs are published in a consolidated way by the MFA, which basically provides the link to the UN consolidated sanctions list both for TF and PF. Therefore, the deficiency in relation to timely transposition of PF related UNSCRs is to some extent mitigated. Other competent authorities, such as the FID-SANS, also provide links to the UN consolidated sanction list. These lists are the main source of conducting checks for those OEs, which do not rely on automated screening solutions. Above mentioned approach does not ensure immediate communication of designations and the amendments to the UN sanction lists of designated

persons and entities to the OEs. This has an impact on the implementation of the relevant UNSCRs by the OEs that do not rely on automated sanctions screening mechanisms.

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

437. Although according to the national legislation OEs, are not obliged to submit STRs in relation to PF, there have been cases of PF related STRs submitted to the FID-SANS (in relation to suspicions on PF or on breaches of proliferation prohibitions/sanctions in general). Main suspicions are related to deals with defence-related products and dual use items which are regarded by the OEs as high-risk products, as well as related to transactions, clients from, geographical regions of proliferation concern or imposed arms embargos (not only Iran and DPRK). The FID-SANS also receives information requests from specialized directorate within SANS in relation to granting licenses for dual use or sensitive goods, or import, export activities which raise proliferation related suspicions. In the period 2014-2020 FID-SANS received and answered total of 14 requests. In addition, the FID-SANS has made 59 spontaneous disseminations regarding counter proliferation STRs and information obtained through international cooperation.

438. There is a robust export control regime targeting proliferation risks in Bulgaria with the central authority being the Inter-ministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction. All competent authorities involved in the export control regime (Counter Proliferation Centre in the State Agency of National Security, Ministry of Foreign Affairs, Ministry of Economy, National Customs Agency and Ministry of Defense and etc.) monitor and check relevant UNSCRs during the process of licensing and after it, and continuously exchange information with one another and the FID-SANS regarding the financial aspects of the export, import deals. Competent authorities have also detected attempts for evasion of sanctions (of proliferation). Most of them were connected with falsification of documents, aiming to misuse the Bulgarian export-control system, as well as the export-control mechanism of other EU countries. Although the mentioned cases were not related to the evasion of UN PF-related TFS, they show the ability of national authorities to identify and detect sanctions evasion schemes involving falsified documents, demonstrated international cooperation arrangements with other involved countries.

4.4.3. FIs, DNFBPs and VASPs' understanding of and compliance with obligations

439. Measures taken by the OEs in relation to TFS to combat PF do not differ from those to combat TF. Thus, deficiencies mentioned in the analysis of IO.4 apply also to the IO.11. Most of the FIs and all VASPs met onsite, rely on automated solutions and commercial databases which contain information on UN consolidated sanctions lists. DNFBPs mostly conduct manual checks through the links to UN consolidated sanctions list provided by the FID-SANS. Some of the lawyers, lack a basic understanding of UN PF related TFS regime and stated that in case of a match with a UNSCR related to PF they would not suspend the provision of services to the client but would report to the FID-SANS. The screening checks are conducted both at the stage of establishing a business relationship and before each transaction. In case of automated solutions, the checks are being conducted on an ongoing basis. In case of manual checks, the screening frequency of an on-boarded customer depends on his/her risk level, which means that a potential match of existing customers with the UNSCR lists would not be identified in a timely manner.

Some of the VASPs mentioned that it would not be possible to freeze funds when fiat is converted to crypto, because of the speed of the transactions. Besides, some of the VASPs, applied various thresholds for identification, which impediment their ability of identifying matches with UNSCRs.

440. On a positive note, the OEs with some exceptions (being some of the payment service providers) stated that the screening against the relevant UN lists covers not only the customer, but also BOs, shareholders, directors, as well as representatives of legal persons, all parties of the transaction. Nevertheless, as provided under IO.4 analysis, the OEs faced issues when identifying the BO of complex structures. Thus, the deficiencies among the FIs and DNFBPs in the identification and verification of BO information reflects on the ability to identify a PF designated person or entity that would be indirectly benefiting from the services provided by these OEs.

441. All OEs, including some of the banks, are concentrated on freezing or blocking funds in a particular transaction, as well as suspension of services to the person who appears in relevant UNSCRs. These OEs do not conduct additional measures for example checks to identify whether the person who appears on the list is a BO or controlling person of another legal entity or customer or if the OE or other customer of the bank holds funds and other assets belonging to listed individual within their institution. A common deficiency among DNFBPs was a confusion between the high-risk countries and TFS regimes and related obligations. Some of the lawyers and accountants, as well as VASPs could not clearly articulate which lists they are actually checking. All DNFBPs mentioned that the TFS related obligations were limited to rejecting the transaction and suspending business relationships, thus there is a lack of understanding of the wider concept of freezing (this particularly concerns the gambling sector) funds and other assets (e.g., legal instruments, contracts, etc.).

442. All OEs, with the exception of some lawyers, mentioned that there would be no difference in their actions if they identify a match with UN resolutions, which is not yet transposed to the EU framework, with the main actions being freezing and suspension of services. All FIs and DNFBPs lack a comprehensive understanding of PF related obligations and consider that PF related obligations are equal only to the screening with the relevant lists.

443. Overall, the awareness and statements of other OEs were based only on the fact that UN lists are being published in a consolidated manner with regard to both TF and PF related resolutions and limited to screening those lists. No training or other awareness raising activities were conducted by the authorities in relation to PF.

4.4.4. Competent authorities ensuring and monitoring compliance

444. All supervisory authorities claimed that although they have no legally defined powers to supervise and sanction TFS obligations in relation to PF, they do check the compliance of OEs with sanctions screening obligations, which *per se* include also PF related UNSCRs. The checks are limited to screening systems and using of consolidated lists and do not look at more wider issues, such as PF related sanctions evasions. As claimed by the authorities no major shortcomings were identified. More detailed analysis of supervision of TFS obligations for PF (as well as TF) is described under IO.3. There was no specific guidance provided to OEs on TFS related to PF, relevant sanctions evasion techniques and PF risks.

Overall conclusions on IO.11

445. Bulgaria implements TFS related to PF through EU regulations and thus is generally impacted by the delays between the designation decision taken by the UNSCs and its

transposition into the EU framework. This is to some extent mitigated by the fact that all UNSCRs are published in a consolidated way by the MFA, which basically provides the link to the UN consolidated sanctions list both for TF and PF. However, this approach does not ensure immediate communication of designations and the amendments to the UNSCRs to OEs.

446. The awareness and statements of OEs, with exception of some banks, were based only on the fact that UN lists are being published in a consolidated manner with regard to both TF and PF related resolutions and limited their obligations to screening those lists.

447. None of the supervisory authorities had legally defied powers to supervise and sanction TFS obligations in relation to PF. At the same time, all of them claimed that they check the compliance of OEs with sanctions screening obligations, which per se include also PF related UNSCRs.

448. **Bulgaria is rated as having a low level of effectiveness for IO.11.**

5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

a) Understanding of AML/CFT legal obligations by OEs is generally high and all those interviewed were aware of the main conclusions of the NRA. Levels of understanding among OEs varied regarding how national risks apply to specific sectors and how individual OEs can be abused for ML purposes: amongst FIs, good understanding was demonstrated by the banks, securities, insurance and VASPs; amongst DNFBPs only real estate agents had generally good understanding, followed by gambling operators and lawyers which demonstrated fairly good understanding. TF risk understanding is less developed for all sectors and is mainly limited to TFS screening obligations and high-risk country lists.

b) All OEs implement risk-mitigating measures including business and customer risk assessments, adherence to cash limitation rules and PEP requirements; however, the scope and nature of these measures vary.

c) General customer due diligence (CDD) and record-keeping requirements are well understood among all OEs, including the prohibition to engage in business where satisfactory CDD was not obtained. Some non-banking FIs and DNFBPs, however, appear to rely to a certain extent on CDD conducted by banks by assuming transactions conducted through banks can be trusted as they are subject to close scrutiny. Some OEs noted difficulties in verifying the ultimate BO of complex structures.

d) All OEs apply enhanced customer due diligence (EDD) measures regarding clients from high-risk countries and PEPs, however, insufficient weighting is given to other situations that could potentially be considered higher risk. In general, the number of customers considered to pose a high risk is low across all OEs, this is especially of concern in the banking sector given its materiality and risks exposure.

e) Although measures are in place by OEs to identify PEPs, information sources used for verification vary. Many of the OEs use a combination of client self-declarations and publicly available commercial or non-commercial databases. Subsequent measures are taken to obtain senior management approval, identify source of funds (SOF) and source of wealth (SOW) and conduct enhanced monitoring. However, difficulties were noted in verifying SOF/SOW and allocating specific (enhanced) monitoring scenarios for PEPs.

f) Varying degrees of application were demonstrated among OEs regarding specific measures for implementation of TFS both in terms of frequency and scope of checks, as well to whom reports should be made in the case of a sanction "hit". None of the interviewed OEs had ever identified "true" matches with the UN TFS lists, nor consulted with the competent authorities regarding potential matches.

g) Although all OEs apply EDD measures with respect to clients from high-risk

jurisdictions, the application of enhanced scrutiny towards transactions to and from high-risk countries varied among banks, payment sector FIs and VASPs. The majority of OEs rely on high-risk countries identified by the European Commission as opposed to the FATF lists.

h) All OEs are aware of the legal requirements to assess the risks related to new technologies, however, they could not articulate any examples of such new technologies (except one bank) with the majority of them claiming that no new technologies had recently been introduced in their businesses.

i) Correspondent banking related obligations and wire transfer rules are well understood by banks and other payment sector FIs. Practical application of wire transfer rules varied between payment sector FIs and the postal remittance sector with some PMOs stating that they still use paper remittance orders when transacting with certain countries.

j) There appears to be a serious issue of under-reporting in most sectors (except banks and some payment sector FIs) mainly due to a lack of knowledge what to look out for in order to identify suspicion. Other than banks, EMIs, PIs and VASPs, most OEs have only a vague awareness of what to look out for to identify suspicion and could not describe the tipping off measures in detail. Transaction monitoring by FIs and the majority of DNFBPs is largely based on thresholds and behavioural scenarios to detect ML and little specific focus is given to scenarios aimed at detecting TF; most could not articulate any examples of TF red flags except for TFS and high-risk countries.

k) All OEs have internal control arrangements to ensure AML/CFT compliance, including internal AML/CFT policies and procedures which are formally adopted at the managerial level, operation of compliance management and control arrangements, and AML/CFT training to employees. The majority of larger FIs have developed multiple lines of defence that also include an independent audit function. Generally, the complexity of the internal control arrangements corresponds to the OEs' size.

Recommended Actions

a) Supervisory authorities should develop sector specific guidance papers and intensify outreach to raise awareness by the private sector on the following topics (in priority order):

i. sector specific "red flags" for transaction monitoring in the area of ML and, separately, TF; as well as typologies of most prevalent predicate offences (incl. tax evasion, corruption, drug trafficking, cash smuggling, human trafficking, etc.)

ii. beneficial ownership (incl. methods to conceal beneficial ownership);

iii. monitoring systems, incl. enhanced monitoring and verification of SOW/SOF, as well as cross-border clients and cross border operations/transactions;

iv. TFS related to TF and sanctions evasion techniques;

v. business wide ML/TF and customer risk assessments, in particular focusing on risk factors used for risk assessment purposes, including assessments of new

technologies such as digital AML/CFT solutions.

b) As the only supervisor with mandate to inspect STR obligations, FID-SANS should target the most material sectors with low STR volumes and those submitting low quality STRs and pay particular attention during onsite examinations to:

i. the robustness of the monitoring systems aimed at detecting separately, ML and TF, that lead to STR reporting;

ii. quality of reporting; as well as raise awareness of the OEs to increase quality of reporting and alleviate tipping of concerns especially given the common practice to freeze or postpone a transaction upon submitting an STR.

c) Supervisory authorities should periodically compare the outcomes of the ML/TF business risk assessments of the OEs, number of clients according to the risk category and STR reporting volumes (as well as feedback from the FID-SANS on the quality of STRs) against the materiality and risk exposure of the OEs and analyse the cases where volumes appear unusual. The most material sectors should be prioritised, namely, banks, followed by other OEs providing remittance services, TCSP services, currency exchange, real estate and VASPs. The outcomes of this analysis should form a part of institutional risk assessments by the supervisors and be subsequently used to allocate appropriate supervisory measures.

d) Supervisory authorities should ensure that the following areas receive priority during on-site examinations (in terms of scope and depth of the checks): business-wide and client risk assessment and mitigation, beneficial ownership, client and transaction monitoring, TFS implementation, high risk countries and PEPs. Special attention should be given to the monitoring scenarios adopted by the OEs during onsite and offsite supervision with a view to assessing whether monitoring systems are sufficiently robust, and risk-based.

e) Supervisory authorities should take necessary actions to ensure that entities are not placing undue reliance on CDD carried out by banks outside of formal arrangements for CDD reliance or outsourcing.

f) Authorities should address the large number of technical deficiencies listed under the Technical Compliance Annex that are relevant to preventive measures, prioritising R.10. Additionally, the country should consider making a risk assessment of all new remote technologies used for client onboarding purposes (identification, verification of clients, in particular focusing on legal persons) and introduce relevant mitigating measures.

449. The relevant IO considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

5.2. Immediate Outcome 4 (Preventive Measures)

Intro & weighting

450. Based on their relative materiality and risk, implementation issues were weighted as follows: most important for the banking sector; highly important for entities providing money value transfer services (payment institutions, e-money institutions, postal service operators[48] that issue postal money orders), currency exchange providers, real estate agents (incl. notaries attached to real estate deals), lawyers and accountants that provide company services and other activities covered by the FATF standard (see c.22.1(d) and (e)) and VASPs; Moderately important for securities and gambling operators; less important for insurance and other types of financial institutions, such as credit co-operatives, leasing and lending.

451. Risk based approach was followed: (i) for the interview process (i.e., when deciding on the number of OEs and sectors that deserve most of the attention; also on the nature, scope and length of the interviews); and (ii) for drafting the analysis (i.e., implementation of the requirements that are considered the most material in the country context were described in greater detail, especially where shortcomings that apply to more heavily weighted sectors have been identified).

452. Reflecting this weighting, the evaluators devoted a considerable amount of time to meeting banks, MVTS, entities providing company formation services and DNFBPs involved in the sale and purchase of real estate (real estate agents and notaries). Meetings were held with 6 banks, 3 payment institutions, 4 e-money institutions, 3 agents of e-money and payment institutions, 2 postal operators, 3 currency exchange offices, 2 wealth management companies, 2 investment brokers, 3 insurance companies, 5 VASPs, 3 other FIs (leasing, consumer loans – fast credits, credit cooperative), 4 lawyers, 3 CSPs (comprising 2 lawyers and 1 accountant), 2 accountants, 2 auditors[49], 2 notaries, 3 real estate brokers, 3 casinos (covering both land-based and remote), and 2 DPMS as well as 4 professional and self-regulatory bodies regarding lawyers, accountants, notaries and private enforcement agents. OEs representing the most material sectors were selected for the interviews based on the nature and scale of the OEs' activities, research through public channels and liaisons with the competent authorities. Several DNFBPs were not able to attend the scheduled interview and therefore were replaced by other entities suggested by the Bulgarian authorities.

453. IO.4 conclusions are largely based on the interviews with the OEs, and to some extent supported by the supervisory data (incl. examination findings) and internal AML/CFT/TFS procedures of the OEs.

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

454. OEs' understanding of AML/CFT obligations is generally high, however, the understanding of ML/TF risks varies across the sectors, with a generally undeveloped TF risk understanding which is common to all sectors and OEs interviewed. The majority of OEs were

[48] For the purposes of IO.4 analysis, postal remittance operators are grouped together with FIs: although they do not have FI status in Bulgaria, in light of the postal money remittance services they provide, their application of preventative measures are analyzed similarly to PIs and EMIs which are authorized to provide MVTS.

[49] None of the auditors met onsite conduct activities that are designated by the FATF standards therefore their responses have not been included.

aware of the main conclusions of the NRA and the related risk events that were relevant to their business. Understanding of risks beyond the NRA is far less developed with only the majority of the banks, securities, insurance, estate agents and VASPs being an exception. Some OEs were able to describe the provisions of LMML, LMFT and RILMML in impressive detail, however, in the majority of cases, OEs were less articulate on how their businesses could be abused for ML/TF purposes and reported very low numbers of high-risk clients which, in some cases, seems at odds with their nature of business and client base. In general, all OEs mentioned corruption and prevalent use of cash among national risks that are also relevant to their businesses.

455. Although business wide ML/TF risk assessments are commonly conducted by the OEs, limited understanding by many OEs of the risks specific to their business calls into question the quality of these assessments. While necessary and beneficial for OEs to have good understanding of the country's NRA, it may not be sufficient, and OEs should understand the ML/TF risks specific to their businesses so they can be addressed through the risk-based application of preventive measures. Common areas of compliance failings identified by supervisors, however, do not include the OE's ML/TF risk assessment.

FIs

456. In general, the banks demonstrated a relatively good understanding of the ML risks to which they are exposed. However, all banks interviewed reported having only a small number of high-risk customers despite some having a relatively high proportion of non-resident clients (noting that this also includes EU clients that typically are not higher risk) and clients engaged in higher risk industries, such as trade finance, dual use goods and maritime fleets registered offshore. Most banks met onsite reported that legal persons established in Bulgaria, especially complex structures with the foreign legal owners, pose the most significant risk to their businesses – this also features as the main typology in STRs submitted by the majority of interviewed banks. The branch of a foreign bank was less articulate about its risk exposure, but this might be due to the small scale of business activities and simple nature of products offered in Bulgaria.

457. In the banking and payment sectors high-risk customers are typically those identified as PEPs or from high-risk third countries with varying degrees of consideration given to other factors that might be relevant. The procedure for risk-assessing customers utilised by one e-money institution was based on allocation of points for various risk factors and a total score over a certain value was considered high-risk. However, the scores for each risk factor were low meaning that a large number of risk factors must be present in order for a customer to be deemed high-risk. Two of the banks met onsite had carried out client base review projects aimed at closing business relationships with certain high-risk customers, thus demonstrating a more conservative risk appetite.

458. Risk understanding varies amongst other FIs. Although representatives of the securities and insurance sectors typically demonstrated a good level of ML risk understanding relevant to their sectors, the payment institutions and e-money institutions do not fully understand the inherent risks of the products and services they offer. One payment institution was unable to articulate a sound economic rationale for their offering of a specific service and one e-money institution was unable to explain why clients, including a relatively high proportion of PEPs, would use their service rather than a bank account. Postal money operators, currency exchange providers and other FIs had limited risk understanding, especially regarding cross-border payments, geographical risks, threats relating to branches close to borders, e.g., cash smuggling,

human trafficking; with the majority not being able to articulate who are the main users of the currency exchange in cash services and how/why these services are relevant for users' businesses (especially in light of high number of large cash transactions exceeding EUR 15 000 and clients with whom a business relationships are formed, as opposed to walk-in clients). Postal money operators and currency exchangers could not articulate how their businesses can be abused for ML/TF purposes.

459. Limited understanding of risks by some payment sector FIs, currency exchangers and postal money operators has a direct impact on their ability to identify suspicious clients and suspicious patterns of transactions. Cross border remittance payments conducted by postal money operators that fall outside of scope of the BNB's licensing and supervision are of special concern.

DNFBPs

460. Gambling operators met onsite were familiar with the NRA and were aware of publicised gambling typologies including, e.g., chip-dumping. They demonstrated reasonable ML risk understanding yet poor TF risk understanding as they did not consider there to be any TF risk; and considered that attempts by customers to defraud the operator (i.e., abuse of bonus offerings, match fixing, etc.) was the biggest risk although in some cases they appeared to describe business or commercial rather than ML risk.

461. Although lawyers demonstrated reasonable risk understanding, each claimed to have very few high-risk clients. Further, there was a suggestion that risky business is carried out by a small number of corrupt firms. Persons that carry out TCSP services demonstrated limited awareness of high-risk scenarios, including the risks posed by PEPs.

462. Estate agents demonstrated good understanding of risks including those that are specific to geographical region and economic climate, stating that due to low living standards some Bulgarian residents may be susceptible to collaborating with international money launderers. However, notaries did not demonstrate good understanding and, despite significant involvement in arrangements for the purchase and sale of real estate, they considered their function to pose a low ML/TF risk.

463. Whilst dealers in precious metals and stones (DPMS) are not classified as obliged entities in Bulgarian legislation due to a prohibition on transactions over BGN 10 000 (approx. EUR 5 000) under the LCPA, they were met by the evaluators to see whether DPMS have any controls in place to comply with the legal prohibitions. The DPMS representatives were aware of the conclusions of the NRA and had a reasonable understanding of ML/TF risk. It was confirmed that they have monitoring procedures in place to identify transactions above the threshold, including linked transactions over the threshold and had made STRs to the FID-SANS regarding cash transactions and instances where customers refuse to confirm their source of funds.

VASPs

464. VASP representatives demonstrated a good understanding of ML/TF risks including specific threats and typologies relevant to their business. Understanding regarding the practical application of AML/CFT requirements was less well developed. Due to de-risking on the part of banks, it was noted as emerging practice for VASPs to engage the services of payment institutions and e-money institutions.

5.2.2. Application of risk mitigating measures

465. Overall, risk-mitigating measures are applied to a good extent. All OEs have implemented procedures for risk assessing their own business and their customers, and apply measures using a risk-based approach, however, shortcomings do exist. Across all sectors, very few customers are considered to be high-risk which, in some cases, does not seem in line with the OEs' range/scale of product offering and customer base. Despite cash limitation rules, large cash transactions are common in banking and currency exchange yet few STRs are reported in this area. Some FIs, gambling operators and VASPs have implemented targeted (enhanced) controls to address ML/TF risk in addition to the legal requirements. In the DNFBP sector, standard rules are implemented by lawyers, notaries and accountants which helps establish baseline level of compliance.

FIs

466. All FIs had established internal procedures for ML/TF risk assessment of their own business and of customers. In the majority of cases, FIs report very low numbers of high-risk clients seemingly at odds with the business activities and customer base described to the AT and when compared to the NRA-identified risks that are relevant to their sectors. When asked the reasons for determining if a customer is high-risk, most described only the scenarios listed in LMML where enhanced CDD is mandatory, namely where the customer or beneficial owner is a PEP or from a high-risk third country (for more information on mitigating measures in relation to PEPs and high-risk countries, please see the section 5.2.4 below).

467. Although FIs had implemented transaction monitoring systems that identify transactions that are large, repeat, complex, etc., the nature of the customer's behavioural activity (i.e. transaction and activities that do not correspond to the usual activities, risk profile, etc.) alone does not appear to be sufficient for the FI to re-consider the customer's level of risk.

468. Sources used to assess high-risk third countries varied among FIs: some utilised EU lists as required by LMML, some utilised FATF or other lists and some used a combination, seemingly led by group policies.

469. All FIs were well aware of the requirement to report cash transactions over BGN 30 000 (approx. € 15 000) to FID-SANS. A number of the banks met onsite had implemented additional measures to control large cash transactions including a requirement to obtain approval of the AML/CFT Unit for very large transactions; or had lowered internal cash transaction thresholds. One bank met onsite had implemented a requirement for manual review (analysis) and approval by higher management of all transactions conducted in foreign currency. However, despite such additional measures, banks continue to report that large cash transactions are commonplace and could not articulate sound economic rationale for this. Comparatively low numbers of STRs are made compared to CTRs and there are cases of violations of reporting requirements identified by the supervisors.

470. Some MVTS providers recognised that they were exposed to being utilised for hawala banking and that money transfers to Turkey, Greece and Arab countries could be for illicit purposes at the same time naming Turkey and Greece as high-risk neighbouring countries. In general, all FIs operating in the payment sector were aware of the issue of unlicensed service providers and hawaladars operating in Bulgaria and reported working with FID-SANS in this regard. However, in 2015-2020, only one STR on potential hawala providers was submitted by the bank and none from other FIs operating in the payment sector (EMIs, PIs and PMOs).

471. Currency exchange providers had not introduced any controls specifically aimed at cash smuggling or human trafficking, including those that had branches located close to borders, and seemed unaware that such issues exist. They did, however, have controls to identify transactions in "exotic" currencies (example cited was Thai Bat to US Dollar) and applied additional measures in such cases. It was suggested by the entities that the EUR 5 000 transaction limit over which CDD is required is not commensurate with the risks and that a lower threshold would be more appropriate. One provider carries out CDD when transactions are near to but slightly less than the threshold in case the customer is aware of and trying to avoid the threshold. It is not understandable, however, that even admitting cash-related risks and suggesting additional mitigating measures for the country, currency exchange operators have filed an insignificant number of STRs in the period under review. For example, in 2019 and 2020 respectively 2 and 3 STRs have been sent by all currency exchangers (almost 2,5 thousand registered persons and some of them having larger client service networks which totals an even larger number of client service locations), while number of CTRs in 2019 and 2020 respectively were 7 205 and 8 820. It is questionable, therefore, that out of 7-8 thousand cash transactions over BGN 30 000 (approx. €15 000) there were not more cases of suspicion being triggered. In addition, currency exchangers provided contradictory views on the profile of their clients and the purpose for which they are using currency exchange services, e.g., some were stating that mainly tourists are using this service, however, could not articulate as to why tourist operate large amounts in cash; some were stating that they have frequent clients that mostly are legal persons with which business relations are established and that engage in import/export activities with neighbouring countries (e.g., Turkey) and real estate developers, however, it was not clearly explained to the assessment team as to why these types of businesses are using currency exchange and transacting in large amounts of cash on a frequent basis.

477. Other FIs (leasing, credit) advised evaluators that third-party loan repayments are not permitted along with the securities firms that confirmed that third party payments are not allowed – which in both cases serves as a mitigating measure.

DNFBPs

478. Gambling operators met onsite had established risk-based AML/CFT controls aimed at mitigating the risks, including, in the case of online gambling, measures to prevent customers from making a withdrawal to a third party and to prohibit customers that are acting by way of business. In some cases, operators applied CDD at lower thresholds than required by the LMML.

479. Lawyers, notaries and accountants met onsite had adopted the uniform internal AML/CFT rules established by the FID-SANS jointly with the professional bodies. The same is applicable for lawyers and accountants who act as TCSPs. Lawyers met onsite described that, due to reputational rankings, firms are selective about the reputation of the clients with whom they engage leading to de-risking.

480. The Bulgarian system for the purchase and sale of real estate requires involvement of a notary. The notary's function includes checking BO information against the commercial register and establishing the SOF for the transaction. It does not extend to establishing whether the sale price (determined based on taxation and not considered to be aligned with true value) is reasonable. This is relevant due to prevalent ML scheme identified in the NRA regarding under-valuing of real estate.

481. Although real estate agents met onsite were performing legal AML/CFT and TFS obligations when dealing with clients selling and purchasing real estate, they also tend to place

indirect reliance on banking checks as an additional control measure especially with regards to SOF/SOW of a client. All real estate agents were in agreement that further regulation, especially in relation to licensing /registration, including establishment of a supervisory body tasked with carrying out entry controls, would be a positive step to also ensure level playing field for the entire real estate brokerage market.

VASPs

482. The VASPS met on site had introduced risk-based AML/CFT controls as required by the LMML/LMFT and in some cases had applied additional measures they considered appropriate, including prohibiting any third-party payments (albeit they recognised significant challenge in cases where payments are made to and from virtual currency) and refusing to do business with customers that are PEPs. VASPs utilise blockchain analytical tools as part of their CDD processes.

5.2.3. Application of CDD and record-keeping requirements

483. FIs and DNFBPs have in place generally good control measures that include all the general elements of CDD and record-keeping,

FIs

Identification and verification

484. Whilst CDD practices are consistent regarding business conducted on a face-to-face basis, measures vary quite considerably, regarding verification of identity of remote clients (although remote clients do not represent large proportion of client base). The majority of FIs utilise one or more third party systems to verify CDD information and documents as well as publicly available Bulgarian databases and actual identity documents, including proof of addresses in some cases. While it is more common to utilise face-to-face onboarding in the banking sector, some banks are about to start utilizing video identification methods and started testing the systems for this reason.

485. Video identification tools are frequently used by some e-money institutions and by investment companies; some other FIs reported they obtain a "selfie" of the potential client holding their photographic identification document. Some payment institutions and e-money institutions obtain CDD via agents and/or couriers (that are not considered to be agents, but nevertheless having a role in an identification process). It must be noted that, while remote identification through digital channels is permitted in the country's legislation, no detailed rules or guidance is available for payment sector businesses on how to utilize some identity verification methods, e.g., through selfie. Fraud cases suggest insufficient capacity of OEs that are using remote identification to mitigate the risks properly, thus, consequently resulting in abuse of their services for illicit purposes.

486. For example, one company providing consumer loans that utilised the "selfie" method advised evaluators that there had been a number of fraud cases where the identity documents of family members had been used. They furthered that in each case the same Bulgarian e-money institution was used indicating that effectiveness of remote CDD measures applied by both, the leasing company and the payment institution, was limited.

Beneficial ownership

487. FIs met onsite were familiar with legal requirements regarding beneficial ownership and exercise of control over the legal persons, including applicable definitions and the prohibition on bearer shares. The practical steps to establish and verify ownership include a combination of

obtaining self-declarations from the client, legal documents (articles of association, etc.) and checking data against the Commercial Register. Some entities had identified discrepancies with data in the register and some noted difficulties in establishing the ultimate beneficial owner in cases where structures are complex.

Incomplete CDD

488. All FIs confirmed that incomplete (missing or unsatisfactory CDD) would result in a business relationship or transaction proceeding no further. None confirmed that they would also consider whether a STR should be filed, however, the authorities cited examples where such reports had been filed. Examples of refusal reasons cited include where a potential client appears to be a shell company. An e-money institution advised the AT that, where complex ownership structures were identified, the relationship would be terminated which indicates that the complete ownership structure may not always be known from the outset. Another e-money institution cited a case where ownership was stated as a family and it was impossible to identify the actual individuals resulting in the business relationship being declined.

Source of funds, nature and purpose of business relationship

489. The majority of FI activity constitutes business relationships and customer KYC questionnaires are used in order to establish the nature and purpose of the relationship. Template document forms are provided as appendices to the RILMML. E-money institutions also require confirmation of the purpose of any third-party payment requests. Currency exchange offices and PMOs also utilise customer declarations regarding business relationships or occasional transactions over BGN 5 000 (approx. € 2 500) and BGN 2 000 (approx. € 1 000) respectively.

Simplified CDD

490. In very few cases, FIs conduct simplified CDD with prior the FID-SANS consent. Examples include payment institutions collecting fees for Government departments. The LMML requires for prior approval of the FID-SANS in order to conduct simplified due diligence. The evaluators were provided with examples of requests made and either agreed, queried or refused. In total 19 requests were made in 2019-mid-2021, 5 of which were refused.

Record-keeping

491. Entities met onsite were aware of legal requirements regarding record-keeping. Minor shortcomings have been identified by supervisors in this area including failure to properly document CDD carried out and not having CDD documents translated into Bulgarian. Paper-based systems remain commonplace within postal money operators which might potentially impact upon ability to monitor customer activity in order to establish repeat transactions under the applicable thresholds for CDD or CTR or suspicious operations.

DNFBPs

492. DNFBP business except remote casinos is predominantly conducted on a face-to-face basis. Practical steps to conduct CDD, including establishment and verification of beneficial ownership, were broadly aligned with measures described by FIs. In cases where the client is not present, video identification is utilised.

493. No DNFBPs met onsite considered that they rely on third parties for CDD purposes other than notaries and real estate agents in cases where they are dealing with proxies that have powers of attorney. However, lawyers described obtaining documents from third parties and raising any issues with documents to the third party rather than directly with the client and accountants

described how they took some comfort in CDD of clients having established relationship with a bank as it was presumed that a high standard of CDD would already have been conducted. Accountants also advised that banks review and approve CDD on shared clients. Thus, although only core principle FIs are permitted to rely on credit institutions for CDD purposes, according to R.17, in practice this is not always followed.

494. Real estate agents (the most material DNFBP sector) apply risk-based CDD measures to a good extent; No serious issues have been identified by the supervisory authorities although the low STR volumes and number of onsite examinations are of concern (see IO3 and IO6 for more information).

496. Land-based casino representatives confirmed that satisfactory CDD is required in order to enter a casino in all cases. Remote casino representatives explained that accounts are opened based on information only, with verification carried out when a customer seeks to make a withdrawal over a BGN 2 000 (approx. € 1 000). This approach is not in line with the LMML, as the threshold also applies to amounts wagered.

497. Lawyers and accountants also described that it is not uncommon for information in the Commercial Register (specifically pointing out to BO information held in the Registry) to differ to information ascertained through CDD conducted and considered that the role of notaries was limited and did not include verifying BO information entered into registers.

498. In most cases measures described by DNFBPs for establishing the source of funds and nature and purpose of activity was limited to information provided by the client in a self-declaration form which might not be sufficient to establish the true origin of the funds in all cases.

VASPs

499. Some VASPs utilise affiliates for the introduction of new customers, however, this does not include participation in, or provision of, CDD. VASPs operate a number of virtual currency ATMs in Sofia, Plovdiv and Varna. The scope of CDD measures introduced by some VASPs depend on the value of transactions, e.g., at lower values for BGN 500 - 2 000 (approx. € 250 – 1 000) only a phone number is required; for BGN 2 000 - 4 000 (approx. € 1 000 – 2 000) identification details with a photograph is required; for BGN 4 000 - 6 000 (approx. € 2 000 – 3 000) a "selfie" is also required; over this threshold (BGN 6 000 or approx. € 3 000) a self-declaration on the additional KYC details (e.g., SOF, purpose and nature of business relationship) is also required. These CDD thresholds are not compliant neither with the requirements under the LMML, nor with the requirements of the FATF standard (see R.15).

5.2.4. Application of EDD measures

Politically exposed persons

500. All OEs apply specific measures regarding clients and beneficial owners that are PEPs and are well aware that the PEP definition extends to family members and close associates, with majority of them admitting that identification of the latter is often a challenge.

501. The vast majority make checks against publicly available information sources provided by the FID-SANS and the CACIAF for domestic PEPs and/or private databases as well as obtaining self-declarations from clients. The screening checks regarding PEP status are usually done both before onboarding and on an ongoing basis (some smaller FIs outsource such customer screening to a bank). World-wide commercial third-party databases are considered by the majority of OEs

that use them as the most comprehensive information source, especially regarding close associates of PEPs.

502. PEP identification and verification mechanisms utilised by some OEs are not fully satisfactory: two lawyers rely entirely on self-declarations made by clients and one payment institution relies upon the local knowledge of couriers[50] to identify customers that are PEPs. As detailed at R.12, Bulgarian law allows OEs to utilise only one of a range of methods to identify PEPs (e.g., the self-declaration), except in cases where the risk is assessed as high (more than one method is required in such cases). VASPs met onsite were unaware of any publicly available sources to assist in verification of PEP status.

503. The number of PEPs serviced by the entities met onsite appears extremely low or zero in those entities who consider PEP clients outside their risk appetite. This could be attributed to various reasons: e.g., policies to de-risk; ineffective practical measures to identify and, more importantly, verify PEPs; narrow application of PEP definition.

504. All OEs operate procedures for obtaining senior management approval in case of business relationship with PEPs, conduct enhanced monitoring and establish SOW/SOF. However, the majority of OEs admitted that sometimes they face difficulties in verifying SOF/SOW information and could not articulate how enhanced monitoring for PEPs is different from usual monitoring.

Correspondent banking

505. Banks apply EDD measures with respect to respondent banks, including consideration of country risks and reputation as well as obtaining senior management approval to establish correspondent relationships.

New technologies

506. Most entities met onsite were aware of the legal requirements to risk assess but could not describe in detail how this would be carried out in practice and could not cite examples of risk assessments already carried out despite, in some cases, recent internal developments such as adopting video identification for remote clients. One bank did, however, demonstrate good understanding and commented on one example where risk assessments were carried out regarding AML software.

Wire transfers

507. Banks and other payment sector FIs are familiar with the wire transfer rules. The destination of the majority of wire transfers are EU/EEA Member States, followed by transfers to other countries, such as China, US and neighbouring countries. It is common to scrutinise wire transfers outside the EU, in accordance with wire transfer rules. One bank stated they carry out manual reviews of all non-BGN transactions that are predominately in US Dollars. However, practical conduct of wire transfers varied between payment sector FIs and the postal remittance sector with some PMOs stating that they still use paper remittance orders when transacting with certain countries. There are no specific virtual asset transfer rules issued in Bulgaria, however, VASPs met onsite were aware of the legal requirements to identify clients and beneficiaries (payers and payees) at the same time admitting that this is not always possible due to the technologies used to execute the virtual transfers. It is common in the VASPs sector to use risk-

[50] BNB suggests that such couriers are agents, however, that did not appear to be the case based on OE interviews.

based thresholds that determine the level of identification until full identification and verification is reached (for more information on CDD conducted by VASPs see chapter 5.2.3 above).

Targeted financial sanctions

508. The majority of entities have a good level of awareness of UN and EU sanctions lists, including the requirement to freeze assets of UN designated entities and individuals although many were not aware of the specific reporting requirements. When talking about TFS related to TF, OEs commonly extend their understanding to high-risk countries.

509. Most FIs had established automated screening systems and apply screening to customers as well as the various parties to a transaction including the remitter, beneficiary, other parties or banks in the chain and to references. However, not all entities operating in the payment sector confirmed that screening was also applied to beneficial owners (incl. signatories and other entities in the ownership chain). One bank stated that automatic screening checks on beneficial owners are performed only when BO details are entered into the system suggesting that BO details may not be screened in every case. Some smaller FIs and DNFBPs were reliant on manual screening checks or had outsourcing arrangements in place.

510. Frequency of checks also vary among OEs. While banks perform screening before client onboarding and at the time of execution of each transaction and/or overnight screening of the entire client database, some other payment sector FIs determine periodic screening intervals based on the client risk level. The same is applicable to almost all DNFBPs, the exception being real estate agents and casinos (excluding online gambling that perform periodic checks based on client risk level) who do not usually maintain a longer-term business relationship with their clients. Periodic checks conducted by some TCSPs depend on client risk level and/or are conducted on annual basis as well as when triggered by change of circumstances (e.g., change of shareholding); one TCSP stated that periodic checks are triggered by enquiries from their partners (other law firms). One lawyer stated they do not perform TFS checks at all.

511. VASPs were aware of TFS screening obligations, at the same time admitting that it is not always possible to screen all the clients, beneficiaries and transactions in the VASPs sector due to the specificities related to the technologies; the precondition to screening by VASPs is to hold full identification and verification of the clients and BO details which are not always available due to identification thresholds.

512. OEs uniformly reported that they analyse partial TFS matches to make a conclusion whether funds and assets belong to UN designated persons and entities. None of the interviewed OEs have ever identified matches with the TFS lists, nor consulted with the competent authorities regarding potential matches which does not seem reasonable given the large number of entities interviewed, including entities with significant number of clients. Awareness of to whom to report in case of sanction hits therefore varied, i.e., some OEs were stating that they would report to the FID-SANS, some – to the FID-SANS and SANS; some were mentioning the FID-SANS and the MoFA; some mentioned MoI; majority of DNFBPs that do not hold client assets has stated that in case of a sanction "hit" they simply would refuse onboarding of the client or cancel the business relationship and were not confirming that they would report a sanction match to the authorities.

513. None of the interviewed OEs with exception of some of the banks, when asked about monitoring systems and red flags, pointed out specific scenarios designed to prevent TFS evasion, however, several OEs were describing monitoring scenarios that would be relevant for TF, such

as transactions with conflict zones and locations at the close proximity to the conflict zones, small transaction amounts to/from these countries.

514. Supervisors have not issued any sanctions for breaches of the TFS related to TF requirements to date; the authorities explained that this is due to the fact that the supervised population demonstrates a good level of compliance, i.e., no severe breaches have been identified to date. Given the shortcomings regarding TFS by some of the OEs identified by the AT, the view of supervisors on the good level of compliance with the TFS requirements by OEs is questionable.

Higher-risk countries

515. All FIs and DNFBPs demonstrated appropriate awareness of their obligations to include country risk when assessing whether a customer poses a higher risk of ML/TF and to apply EDD measures to customers from high-risk third countries. However, measures related to the transfers executed *from* and *to* high-risk countries are less well developed and there is a lack of evidence to justify that enhanced monitoring scenarios are applied by payment sector FIs to scrutinize such transactions, except in the case of banks as confirmed by the BNB. While it is often the case that the EU Commission list (hereinafter – EU list) encompasses all of the countries listed by the FATF with North Korea and Iran always being also on EU list, the majority of interviewed OEs (banks being an exception) were not mentioning the FATF lists in the first place but pointing only the EU list (these lists are published on the FID-SANS website and periodically renewed). Only when specifically asked about FATF lists, majority of the OEs confirmed the awareness of those.

516. Most banks and larger FIs go beyond the aforementioned lists and have established internal high-risk country lists based on a range of information sources (i.e., EU lists, FATF lists, Basel AML Index) as well as reflecting solo entity or group risk appetite. In addition, some banks, smaller FIs and CSPs, including lawyers and accountants advised that they pay particular attention to the countries that are considered offshore jurisdictions; this is mainly due to tax compliance purposes. In many cases entities stated that they would not enter into business with customers from high-risk countries as this fall outside of business risk appetite. Those that did accept customers from high-risk countries advised that these are typically Syrian nationals residing in Bulgaria, e.g., students.

517. Measures described regarding customers from high-risk third countries include additional CDD (e.g., a greater scrutiny on identification and verification), establishment of source of wealth/funds as well as enhanced ongoing monitoring of the customer behaviour and transactions. However, entities did not clearly articulate how monitoring of customers from high-risk countries and transactions varied. Several of the AML/CFT internal documents of the OEs reviewed by the AT (with a view to confirm the conclusions on preventive measures in relation to high-risk countries) did not clearly articulate how monitoring was more frequent or more detailed[51].

518. VASPs, in addition to EU listed countries, apply enhanced CDD to customers from other countries that according to their internal assessment are considered to pose a high risk

[51] In the case of banks which is the most material sector, more detailed information on monitoring is included in other documents separate to the main AML/CFT Manual and risk-based monitoring does occur in practice, as confirmed by BNB supervision.

specifically regarding cybercrime; however, challenges were noted in identifying the country of source and destination of payments made in virtual currencies.

519. All OEs stated they had zero or a very low number of clients from high-risk countries and/or seeing transactions with high-risk countries; except those OEs whose internal classification of high-risk countries goes beyond European Commission or FATF lists (mainly banks and some payment sector FIs).

Other high-risk scenarios

520. Generally, OEs described having a very low proportion of high-risk clients including those that offer higher risk products, services or have higher risk clients. Enhanced measures are mostly applied to customers that are PEPs or customers from high-risk third countries with a limited consideration given to other circumstances that might constitute higher risks. Gaps in OE's understanding of risks that are specific to their business also have an impact on ability to properly identify additional higher risk scenarios.

521. It is clear that additional and sector-specific guidance is required to assist entities with identifying circumstances beyond PEPs and high-risk countries that poses a high risk. This is particularly important for the most material sectors with low STR volumes.

522. In some cases, OEs did consider particular activities such as private banking or remote customer relationship as potential indications of high risk. No situations were described where other risk factors would be sufficient grounds to determine high-risk such as particularly large or complex operations, complex beneficial ownership, higher risk business activities, etc. However, the authorities advise that STRs do include such triggers and, moreover, the evaluation of the OEs' monitoring practices forms part of the supervisory assessment of the FIs as reported by the BNB.

5.2.5. Reporting obligations and tipping off

523. All OEs were well aware of the requirement to file an STR to the FID-SANS regarding ML/TF suspicion including the requirement to postpone/delay the transaction(s) and not to tip off the customer, although understanding of which additional authority should be the recipient of STRs related to knowledge of TF varied.

524. With the exception of banks, payment institutions, e-money institutions and postal money operators, STR volumes appear extremely low and virtually no reports are made by other entity types regarding TF suspicion (please see STR reporting statistics under IO6). Although the number of STRs submitted by the MVTS sector - payment institutions and e-money institutions – is relatively high, this does not indicate good quality, as the reporting practices by this sector are described as defensive (see IO6 for more information). Bulgarian authorities advised that in some cases STRs relate to transactions involving other OEs that have not filed an STR, which reinforces the view that there is under-reporting in sectors other than banks. A precondition to file an STR is awareness of risks to which individual entities are exposed, vulnerabilities to ML/TF abuse of their products and services as well as knowledge on typologies and red flags. However, as already noted above (see risk understanding and mitigation sections), many OEs do not demonstrate sufficiently developed understanding in these areas.

525. Volumes of STRs submitted by certain entities met onsite did not appear commensurate with their business activities. For example, one bank reported a high number of large cash transactions (600-700 per month), could not clearly articulate, however, sound economic rationale for this yet had reported few STRs. The doubtful rationale put to the evaluators was

negative interest rates and fees for making transfer which are higher than for withdrawing cash. In general, transaction monitoring by FIs and the majority of DNFBPs is largely based on thresholds and to some extent on behavioural scenarios to detect ML and very little to no specific focus is given to scenarios aimed at detecting TF. Most OEs could not articulate any examples of TF red flags except for TFS and high-risk countries. Common reasons for filing an STR include incoming and immediately outgoing transfers, commonly made by Bulgarian companies with foreign owners, tax crimes, fraud, including phishing attacks and cash transactions with no apparent economic rationale.

526. Based on interviews with the OEs, examples of internal AML/CFT procedures of those interviewed and legislative requirements, the AT considers that a wide range of factors are likely contribute to low report volumes: (1) Lack of awareness of risk factors and "red flags" relevant to their business, particularly regarding TF. None of the OEs met onsite, neither banks confirmed that they allocate specific monitoring scenarios to detect TF as distinct from ML. This is supported not only by interviews, but also internal AML/CFT procedures of OEs reviewed by the AT. In the majority of the cases, transaction monitoring regarding TF appears limited to simply checking sanctions lists and consideration given to clients from high-risk countries. In one example of internal AML/CFT procedures of non-bank payment sector FI, the red flags were fraud related rather than ML/TF; (2) Lack of understanding of risks to which individual businesses and sectors are exposed, beyond national risks; (3) Transactions or relationships are refused by some OEs in cases where satisfactory CDD is not obtained, however, consideration is not given to whether suspicion has been formed by entities other than banks; (4) Internal documents by the OEs provide examples of "red flags" that are overly exaggerated or "high threshold" to meet or require multiple flags to apply in order to be classified suspicious; (5) Limited individual feedback given to OEs by the FID-SANS after filing an STR and/or consolidated feedback on quality, typologies, etc.; (6) Limited supervisory guidance other than EBA guidance for financial sectors on identifying suspicion, red flags, typologies and further guidance on conducting comprehensive business wide and client risk assessment and, subsequently, adopting additional risk mitigation measures.

527. Although all entities were well aware of prohibition to tip off the customer, legal requirements to postpone/delay transactions could elevate potential concerns of tipping off. Some of the FIs that have submitted STRs in the past could not articulate that they have a convincing answer for the customer in case he/she is concerned with a transaction not going through, e.g., some providing explanation that they had technical difficulties in executing the transaction; some explaining that in contractual obligations to the client FIs have reserved a right not to execute a transaction in some cases.

528. The FID-SANS is the only supervisory authority that has legal powers to supervise suspicious activity reporting. A total of 31 instances of non-reporting were identified by the FID-SANS in 2015-2019 and no cases in 2020-2021. The low number of instances identified is not commensurate with the risk exposure of most sectors.

529. The lack of reporting and significant gaps in understanding of what to look out for in order to identify suspicion points to the urgent need for guidance by the supervisory authorities to develop OEs understanding on how ML and TF can occur in the individual OEs, as well as sector and sub-sectors they are representing. However, the vast majority of OEs were uniformly stating that legal requirements are very clear and no further guidance is needed from the authorities. Some minor exemptions are that some OEs pointed out a significant lack of guidance, contradictions between LMML and some other non-AML legal acts, although this view is not

supported by the authorities. One entity stated that if the FID-SANS would tell them to report, they would - which proves the need of a more guidance for the private sector to increase STR reporting.

530. A large number of entities met onsite commented that online reporting mechanisms for both CTRs and STRs would be welcomed. VASPs representatives suggested that there should be a campaign for public awareness regarding scams sites targeting Bulgarian clients to invest in cryptocurrency.

5.2.6. *Internal controls and legal/regulatory requirements impending implementation*

531. Internal controls in OEs to ensure compliance with the AML/CFT requirements include an AML/CFT function or so called "specialised service"[52]. The Head of the Specialised Service performs the function of ML/TF Reporting Officer. All OEs have documented internal procedures and examples provided to the evaluators confirmed that they are regularly reviewed, updated and approved by the senior management. OEs were aware of changes that had been made to AML/CFT laws and regulations during the reporting period, most notably changes to the LMML in 2019, and had updated their internal rules accordingly. Training is provided to new staff, in the event of material changes to AML/CFT requirements and periodically thereafter. Some have established testing requirements to ensure that staff have fully understood the training. However, given the monitoring and STR reporting shortcomings, it is doubtful whether the OEs' internal AML/CFT trainings and internal policies and procedures address client and transaction monitoring effectively.

532. Most banks and other larger entities have appropriate compliance arrangements, incl. group-wide arrangements; had established multiple lines of defence, internal audit, as well as periodic reporting to senior management on AML/CFT matters; also employ technological tools to serve AML/CFT implementation, such as automated systems for identifying PEPs and persons subject to TFS and transaction monitoring.

533. Smaller entities including most DNFBPs have internal policies and controls that are commensurate to the size and risk of their business. They uniformly confirmed having internal AML/CFT rules, performing initial and refresher trainings for staff and at least some arrangements to test internal control systems. However, in small OEs, the function of specialised service is typically carried out by a person that also has commitment to other aspects of the business which may potentially lead to actual or perceived conflict of interest. For example, the ML/TF Reporting Officer may perform control checks on AML/CFT measures that they have carried out themselves. In more severe cases a person with responsibility for attracting new clients could also be responsible for carrying out satisfactory CDD/EDD.

534. Agents of payment institutions and e-money institutions are generally included into the internal control framework of a payment or e-money institution, i.e., this includes requirement to comply with the OE's internal rules, provision of AML/CFT training and measures implemented to ensure compliance. One such entity described a process where "secret shoppers" tested agents. However, one e-money institution interviewed whose agent was a bank appeared to rely on

[52] See Technical Compliance Annex, R.18

internal controls adopted by the bank rather than require the bank to implement the OE's own controls.

535. OEs that are part of the group commonly rely on the internal control arrangements adopted at a group level, including group audit function. Despite the shortcomings noted under R.18, all OEs belonging to a group, uniformly stated that there is nothing that inhibits information sharing between group entities, even on clients and STRs.

Other matters

536. The AML/CFT legal framework in Bulgaria is relatively chaotic. The main laws on AML/CFT - namely the LMML, LMFT and RILMML - apply to all OEs and European guidance applies to certain FIs, creating multiple layers of (sometime contradictory) requirements. This might have an effect on the OEs ability to comply, especially relevant for the new businesses recently introduced into the regulated market, such as VASPs, or other newly licensed entities. This, combined with the significant lack of guidance (see R.34 for more information), might have a negative effect on the overall implementation of the AML/CFT legal requirements. Moreover, supervisory data (including the level of the severity of the supervisory findings and subsequent remedial actions/sanctions) and observations on the compliance trends by the OEs cannot be always evidenced by the reliable and comprehensive supervisory statistics for some sectors (for more information please see IO.3).

537. A number of technical compliance issues might impede the implementation of the preventative measures, as noted in the Technical Compliance Annex. However, none of the reporting entities referred to the limitations in applying the legal requirements and/or circumstances which would lead to the application of the requirements to a lesser extent than required by the FATF standard when compared to the national legal requirements.

Overall conclusions on IO.4

538. Knowledge of AML/CFT legal obligations by OEs is generally high and all OEs conduct general CDD on their clients. Awareness of national risks is developed to a good level by all OEs, however, understanding of risks common to the OEs' businesses is less nuanced. Generally, banks, securities, insurers, VASPs and real estate agents (representing large proportion of the more material sectors) demonstrate reasonable understanding; however, this is an area requiring significant improvement for other payment sector FIs and most other DNFBPs. TF and TFS risk understanding is commonly less well developed than that of ML risk understanding. Linked to this, area of mitigation requires further improvement: although all OEs report having risk mitigating measures in place (incl. business wide ML/TF risk assessment, client risk assessment), degree and scope of these vary amongst sectors.

539. Although implementation of general CDD requirements is generally good among all OEs, enhanced CDD measures are mainly focused on clients from high-risk countries and PEPs with less consideration given to other high-risk circumstances. Linked to this, limited ability of the OEs to identify suspicious activities and transactions by allocating monitoring scenarios to detect ML and TF translates into the low reporting rates; although is less common to the most material sectors – banks and MVTS. Internal controls in the area of AML/CFT compliance are developed in all OEs; generally, the complexity of the internal control arrangements correspond to the OEs' size.

540. **Bulgaria is rated as having a Moderate level of effectiveness for IO.4.**

6. SUPERVISION

6.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 3

a) The FSC and the BNB apply controls to prevent criminals from owning or controlling banks, payment and e-money institutions and entities operating in the securities and insurance markets, however, processes for the identification of close associates of criminals and ongoing monitoring with the licensing requirements require improvement. No criminality or other fit and proper tests are performed regarding virtual asset service providers, postal money operators or shareholders of currency exchange offices. Licensing authorities do not cooperate with the domestic authorities and foreign counterparts in all cases.

b) In the DNFBP sector lawyers and notaries are subject to criminality checks, whilst real estate agents are not subject to any and the obligation to register cannot be enforced. There is no registration regime for TCSPs or accountants.

c) The NaRA has recently been assigned responsibility for entry controls of the gambling sector. Due to well publicised issues surrounding the former regulator, there is no continuity of staff members and a lack of information regarding activities previously undertaken. Therefore, there is a concern whether entry controls previously conducted can reasonably be relied upon. The ownership threshold that triggers *fit and proper* checks is higher than is permitted by the FATF standard and no mechanisms for foreign cooperation have been established.

d) The primary AML/CFT supervisor, the FID-SANS, is knowledgeable about the general ML risk events the country is facing, however, it has limited understanding of threats and vulnerabilities in the supervised sectors and different types of institutions and could not articulate how the risks can manifest. Risk understanding in the DNFBP sector is less developed when compared to the financial sector. Risk understanding is severely hampered by a significant lack of resources, incl. absence of IT tools which does not allow for proper management and use of supervisory data.

e) The BNB and the FSC have a fair understanding of the ML risks present in banking, securities and insurance sectors, however, the risks and vulnerabilities in the non-banking payment sector are understood to a lesser degree.

f) The NaRA seems to underestimate the risks in the currency exchange and gambling sectors whereas the CRC was unable to articulate risks relating to postal money remittance. There is a lack of clarity regarding the remit and legislative powers of the NaRA (regarding currency exchange) and the CRC to conduct supervisory activities.

g) TF risk understanding among all supervisory authorities is not sufficiently developed, especially in relation financial flows and clients by geography. Authorities do not sufficiently focus on TF during onsite examinations; to date, no breaches of the LMFT (which includes TF prevention and TFS requirements) have been detected.

h) Although financial supervisors have mechanisms in place to assess the risks of the supervised sectors, the risk assessment processes need enhancement. The FID-SANS has also established formal processes to assess the risks in some financial sectors, however, there is insufficient evidence that the assessment tools are used in practice in all cases. There are no offsite risk assessment processes regarding the DNFBP sectors which significantly hampers the timely identification of risks in these sectors and does not allow for targeted supervisory measures.

i) Supervisory authorities' internal processes to assess monitoring of TF-related TFS by the supervised entities are not sufficient. No severe breaches have been identified therefore no sanctions have been issued regarding TF-related TFS requirements to date.

j) The intensity and frequency of supervision is not determined on a risk sensitive basis by some supervisors; the FSC's and the BNB's processes are risk based to a good extent but require further enhancement.

k) Whilst financial institutions are subjected to more frequent on-site supervision when compared to DNFBPs, there is an overlap of supervisory powers shared between some authorities and the FID-SANS which, at times, translates into inefficient use of resources by both the supervisors and the supervised entities. Inspections by the CRC have limited effectiveness as they extend only to offsite reviews of internal procedures. Few inspections have been carried out regarding DNFBPs.

l) Regulation and on-site supervision of VASPs are in the infancy stage and no on-site supervision has been conducted to date.

m) In general, the sanctioning regime appears to be overly complicated. Although the FID-SANS has powers to issue sanctions for AML/CFT breaches, the powers to issue sanctions vary among other supervisory authorities. There is a lack of feedback and statistics regarding cases referred to/from the FID-SANS for application of financial penalty/regulatory sanction.

n) The sanctions imposed are often not proportionate, effective and dissuasive. There is a prevalence of court cases whereby penalties were cancelled or reduced. Instances were noted where supervisors described infractions as being minor, whereas the AT considered them to be more serious based on the inspection reports.

o) Supervisors have demonstrated impact on compliance by OEs to a limited extent. Some instances of repeat infractions were noted regarding certain OEs and common violations per sector are noted by the FID-SANS throughout the

reporting period.

p) There is a lack of sector specific guidance to promote understanding by OEs of AML/CFT obligations, especially related to monitoring and identification of suspicious activities/transactions except for EBA guidance.

q) The FID-SANS, the CRC and the NaRA lack the necessary resources (access to relevant information, staff, IT tools) to effectively conduct AML/CFT and TFS supervision. The BNB and FSC would also benefit from additional IT tools.

Recommended Actions

Immediate Outcome 3

a) Authorities should enhance the entry controls regime:

(i) Legal basis and formal regulatory mechanisms should be established for conducting fitness and propriety checks on VASPs, postal money operators, accountants and real estate agents; and shareholders of currency exchange offices;

(ii) Market entry regime should be introduced for TCSPs;

(iii) Beneficial ownership threshold that triggers fit and proper checks for gambling operators should be aligned with the requirements of the FATF standard; The NaRA should conduct checks to either re-examine entry controls previously conducted by the former supervisor or to conduct its own entry controls on gambling operators licensed by the former supervisor;

(iv) Clear legal basis for refusal of application for licence/registration/ownership/control should be established for cases where the applicant is a close associate of a criminal; and formalised internal processes should be developed for identification of close associates of criminals;

(v) Formalised internal processes should be established regarding ongoing monitoring with the licensing requirements;

(vi) Formal mechanisms for cooperation should be established with domestic competent authorities and foreign counterparts regarding all cases of licence applications and changes to ownership and control;

(vii) Formal procedures should be established to identify unlicensed activity on an ongoing basis, including by taking proactive measures.

b) Bulgaria should increase resources in all supervisory authorities:

(i) Technological tools should be introduced to aid data analysis and risk assessment for the most material sectors; as well as to assist in supervisory activities

(ii) Sufficient budgetary resources should be allocated to make sure supervisory staff possess the necessary AML/CFT knowledge and

expertise (the CRC and the NaRA should be prioritised)

(iii) Human resources tasked with AML/CFT supervision have to be urgently increased in the FID-SANS; other supervisory authorities that have not disclosed information on AML/CFT organisational/structural set up and resourcing, should conduct a self-assessment on the sufficiency of the level of staff and appropriateness of the structural and organisational set up of the AML/CFT supervision.

c) Authorities should strengthen the existing, and establish new supervisory risk assessment processes taking into account country, sector risks and risks to which individual supervised entities are exposed:

(i) The existing risk assessment processes utilised by the BNB and the FSC have to be further improved with a greater focus on comprehensively assessing the inherent risk and revising the entire risk calculation method;

(ii) Risk assessment processes for DNFBPs, VASPs and PMOs should be established;

(iii) All supervisors should establish mechanisms for routine collection/sharing of data for AML/CFT risk assessment purposes;

(iv) Supervisors should establish clear methodologies for determining entities that are to receive joint supervision and avoid duplication of efforts in cases, e.g., where FID-SANS and supervisors are separately requesting information to risk-assess the entities;

(v) Supervisors should conduct an exercise (and review this data periodically) to establish how many lawyers, accountants and other legal professionals conduct the activities covered by the FATF standard. This will enable authorities to carry out more targeted supervisory actions.

d) Supervisors should establish effective processes to ensure that the frequency and intensity of supervision is determined on the basis of risk. Supervisory measures should not be limited to onsite checks only; other additional forms of supervisory monitoring and engagement should be considered, in accordance with risk exposure.

e) Frequency, scope and depth of onsite examinations should be urgently increased in DNFBP sectors (priority given to higher risk sectors and higher risk entities in a particular sector), VASPs and PMOs. Financial supervisors should increase the scope and depth of the onsite checks.

f) All supervisors should establish clear mechanisms for monitoring compliance by OEs with TFS requirements both offsite and onsite. As part of this, entities with greater exposure to TFS risks should be identified, and, consequently, should be prioritised for on-site examinations. The scope and depth of on-site checks regarding TFS related to TF should be increased.

g) Supervisory authorities should enhance TF risk understanding of the various supervised sectors through more refined data collection including geographical data on clients, delivery channels and financial flows. Authorities should put more emphasis on TF during onsite examinations; and make sure severe, systemic and repeated

violations are proportionally sanctioned.

h) All supervisors should have explicit legal basis for supervisory powers to monitoring checks on compliance with STR requirements.

i) An effective, proportionate and dissuasive sanctioning regime for AML/CFT and TFS related to TF breaches should be established:

   (i) Proportionate and dissuasive sanctions for dealing with non-compliance should be available to, and utilised by, the supervisory authorities. Domestic cooperation should be improved to provide feedback regarding violations identified and referred to other agencies for sanctions to be applied in cases where the inspecting authority is not the sanctioning authority;

   (ii) Supervisors should examine cases where sanctions have been removed or reduced by court ruling in order to identify and address any procedural shortcomings;

   (iii) Supervisors should develop comprehensive sanction application procedures to ensure the level of sanction is appropriate in accordance with the (i) severity, (ii) systemic and (iii) repeated nature of the breaches.

j) Consolidated supervisory feedback on commonly identified ML/TF breaches should be established; the most common breaches should inform the outreach themes and themes for additional guidance papers. In addition, the need for sector specific guidance is prescribed under IO4.

541. The relevant IO considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26 - 28, 34, 35 and elements of R.1 and 40.

6.2. Immediate Outcome 3 (Supervision)

Materiality and weightings

542. Based on their relative materiality and risk, implementation issues were weighted as follows: most important for the banking sector; highly important for entities providing money value transfer services - namely payment institutions (PIs), e-money institutions (EMIs), and postal service operators that issue postal money orders, referred to as PMOs; as well as currency exchange providers, real estate agents (incl. notaries involved in real estate deals), lawyers and accountants that provide company formation services and other activities covered by the FATF standard (c.22.1(d) and (e)) and VASPs; Moderately important for securities and gambling operators; less important for insurance, other types of financial institutions under the LCI such as credit co-operatives, leasing and lending.

543. When determining the materiality and risk of the sectors and consequently the weightings allocated to them, the assessment team took into account the conclusions of the NRA on the sectorial risks, information on the size, scale and nature of the activities by the sectors and the regulatory vulnerabilities, e.g., market entry measures (or absence of such), comprehensiveness of the supervisory arrangements to monitor compliance with the AML/CFT and TFS-related to TF requirements. See Chapter 1 for more information.

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

544. Overall, licensing, registration and controls preventing criminals and associates from entering the market are effective to a large extent regarding financial institutions regulated by the BNB and the FSC, however, there is no clear legal basis for grounds to refuse applications due to criminal associations. Entry controls regarding PMOs, currency exchange providers, gambling operators, real estate agents, accountants and VASPs require either establishment or significant improvement; there is no market entry regime for TCSPs.

Bulgarian National Bank – banks, PIs, EMIs and other FIs

545. Banks, PIs and EMIs are licensed by the BNB; other FIs (under Art. 3a LCI), including leasing, financial guarantees and lending, are subject to registration. Controls apply both at licence application and in the event of change in ownership or control.

546. In all cases, applicants including managers and shareholders must complete detailed questionnaires aimed at assessing fitness and propriety, as well as declarations regarding criminal convictions and source of funds. BNB staff have access to the criminal convictions database maintained by the MoJ in order to verify declarations. For foreign applicants, certified non-conviction certificates are required. The BNB routinely seeks information from the NaRA and from the FID-SANS to verify source of funds and source of wealth information declared by the applicant. Since 2015, the BNB has made 20 entry controls enquiries to the FID-SANS that relate to 25 PI/EMI applications.

547. Regarding banks, in accordance with the LCI and BNB Ordinance No.2, prior approval is required for holdings that exceed 10 per cent. Notification of holdings over 3 per cent are required as well as declarations regarding fitness and propriety. Although no new banking licences were issued during the reporting period, there were a number of applications regarding changes in ownership and control. In two cases, the BNB refused applications for increasing qualifying holdings although these instances did not raise ML/TF concerns. One bank met onsite had been the subject of various news articles including allegations of improper conduct and links to organised crime and corruption. Whilst the bank disputed the unsubstantiated claims, it noted that the BNB had not sought any clarifications from the bank in this regard.[53]

548. Regarding PIs and EMIs, in accordance with the LPSPS and BNB Ordinance No. 16, the BNB conducts fitness and propriety checks on the persons managing and representing the entity as well as persons with a qualifying holding. During the reporting period, out of 25 PI/EMIs applications received, 12 were refused due to failure to submit required data and documents and 1 application was withdrawn.

549. Other financial institutions[54] listed under Art.3a LCI (leasing, financial guarantees and lending) are subject to registration in a public registry. Although less onerous than the requirements on banks, PIs and EMIs, other FIs must also satisfy requirements regarding the

[53] The bank in question was the subject of a joint AML/CFT inspection in 2020 where no violations were identified, and the bank was rated *medium risk.* The same bank was also subjected to a targeted prudential inspection due to negative media publications from late spring 2021 regarding controversial loan origination practices that were pointing to the issues relating to internal governance arrangements.

[54] AML/CFT supervision of other FIs conducted by the FID-SANS.

fitness and propriety of managers, representatives and qualifying shareholders and of the origin of funds.

Financial Supervision Commission – securities and insurance

550. Entities operating in the securities and insurance sectors are licenced by the FSC. Entry controls apply both at the licence application and in the event of change in ownership or control. Persons with criminal convictions are prohibited from being managers, representatives or persons holding a qualified shareholding in the various regulatory laws (MFIA regarding securities, CISCOUCIA regarding collective investment schemes, IC regarding insurance operators and intermediaries and SIC regarding pension insurance). The following databases are used to verify the information on the applications: the criminal convictions database maintained by the MoJ, the register of bank accounts maintained by the BNB, the Unified Citizens Register[55], the European Securities and Markets Authority (ESMA) sanctions register and they utilise Bulgarian real estate and property registers.

551. Excluding insurance brokers, the FSC has received a total of 92 and refused 19 licence applications during the licensing period comprising of: 27 investment companies (16 refused), 23 alternative investment fund managers, 38 collective investment schemes, 4 management companies (3 refused).

552. The FSC routinely cooperates with the FID-SANS, foreign supervisors and the BNB regarding licence applications. The FID-SANS reports a total 48 requests made by the FSC during the reporting period.

National Revenue Agency – currency exchange offices, gambling operators and VASPs

553. The NaRA is tasked with issuing licences for gambling operators (incl. casinos) and registering currency exchange offices and VASPs.

Currency exchange offices

554. Ordinance No.4 on Bureaux de Exchange prohibits persons with convictions from being registered as individual traders or members of the management or supervisory bodies of an exchange bureau. Non-conviction certificates are required for the representative and for directors, but not for shareholders. None of the 168 applications for registration, nor 47 applications for change of management have been refused during the reporting period.

Gambling operators

555. Following the amendments of the Gambling Law, in August 2020 responsibility for entry controls and supervision of the gambling sector has been transferred from the abolished former regulator, the State Commission on Gambling (SCG), to the NaRA. The Gambling Law lists scenarios whereby a licence shall not be granted and includes where an owner, partner or shareholder with qualified interest (33 per cent), manager, member of a management or controlling body of a company or non-profit legal entity has a criminal conviction. The qualifying threshold for ownership is higher than permitted in the FATF standards.

[55] The register established in Bulgaria includes identification details, name and nationality of immediate family members including spouses and name changes.

556. Despite concerns regarding the effectiveness of the former gambling regulator[56], the SCG, licence holders were not required to reapply for licences and during the onsite it was confirmed that there were no plans to re-check previous entry controls. The NaRA was not able to elaborate on the fit and proper checks carried out by the previous regulator the reasons being that no employees of the SGC were transferred to the NaRA and no internal policies, procedures or instructions on licencing or on supervision previously used by the SCG have been made available to the new regulator (NaRA).

557. No statistics have been provided to the AT regarding applications made, withdrawn, approved or withdrawn during the review period. However, during the onsite meetings the AT was advised that no new applications had been processed since the NaRA assumed responsibility for gambling supervision although a small number of applications that were already underway were completed. The NaRA had not yet entered into agreements for foreign cooperation with other supervisors despite having online gambling operators that are part of international groups and confirmed no ability to check for criminal convictions other than requesting notary-certified criminal conviction certificates.

558. Virtual assets service providers (VASPs) are not subjected to any market entry controls, incl. fitness and property checks; registration neither can be enforced, nor the NaRA does have legal powers to revoke a registration. Ordinance No. H-9 of August 2020 sets out the terms and conditions for entry in the register of persons who provide exchange services between virtual and fiat currency. Entry in the register is prohibited where a sanction has been imposed under LMML/LMFT within the previous 2 years. VASPs met onsite advised that registration is mainly voluntary and there is no level playing field in Bulgaria for VASPs. As at 31 July 2021, 26 VASPs had requested registration with the NaRA.

Communications Regulation Commission - postal service operators

559. PMOs are licenced by the CRC under the Postal Services Act. The CRC may refuse or withdraw a licence only in limited scenarios: threat to national security, bankruptcy, liquidation, etc. There is no legal basis for refusing or revoking a licence due to concerns over fitness and propriety. The AT was advised that information is requested from SANS, the MoD and public registers to assist with licensing checks. The CRC does not undertake any criminality checks regarding the owners and controllers of an applicant and is entirely dependent on other authorities notifying the CRC of an issue. 19 new PMO licenses has been issued during the reporting period and one application refused on the basis of information from SANS and the Ministry of Interior that indicated a threat to national security.

Other DNFBPs

560. Real estate agents are not subject to licensing and registration requirements and do not have an effective self-regulating mechanism. Persons with a conviction are prohibited from entering the market under the LMML, however, no authority is tasked with supervising or enforcing the prohibition.

561. Lawyers and notaries are legally prohibited from being registered in cases where the person has a conviction, see R.28. Checks on conviction status are carried out by the MoJ

[56] Well publicised bribery case, subsequently resulting in resignation of the Chairman of the SCG and dissolvement of the former regulatory authority. As a consequence, due to the criminal allegations, no employees of the SCG have been transferred to the NaRA.

regarding notaries, as these are state appointments; no registrations of notaries[57] were refused during the reporting period. Checks on lawyers are carried out by the Supreme Bar Council and checks on auditors by the Commission for Public Oversight for Registered Auditors. These authorities do not have direct access to the MoJ systems to verify convictions certificates, however, they explained that verification can be done by contacting the MoJ in cases where there is a concern.

562. There is no body with the remit to check that persons entered in the Commercial Register as an accountant are fit and proper persons.

563. Trusts and company service providers (TCSP) are subjected to no licensing or registration regime. Authorities report that, in practice, TCSP services are carried out by the lawyers and accountants. There is no formal specialisation of the lawyers and accountants; and their activities are not limited, therefore, the population of the lawyers and accountants that carry out activities covered by the FATF standard is not established.

Identification of criminal associates

564. There are no explicit regulatory measures in place by the licensing authorities to detect associates of criminals so to prevent them from holding, or being the beneficial owner of, or holding a management function in FIs or DNFBPs, except in the case of the BNB.

565. The BNB, as part of its entry controls, considers a wide range of information sources including information from applicants in the relevant forms, additional information that may be requested from the applicant, the FIU, other Member States' competent authorities and database/software searches. As detailed in the R.26 information, is collected on associates, however, the law is not clear that this may be grounds for refusal, i.e., there no explicit legal basis for any supervisor to refuse a licence, registration or change in ownership and control due to association with criminals exists.

566. In addition, the BNB has established a close cooperation mechanism with the ECB that encompasses measures to prevent criminals and their associates from becoming owners and controllers of a credit institution. In practice, this goes some way to mitigate the absence of clear legal basis, especially in relation to licensees in the banking sector due to formal cooperation with the ECB on these matters. There are no cases where checks have identified criminal associations and thus there are no refusals by the BNB either at application or as part of ongoing checks. However, towards the end of 2020, due to concerns over the source of funds for a proposed acquisition of a qualifying shareholding in a Bulgarian bank, the BNB and ECB discussed the application and enhanced scrutiny was conducted. Following this the application was withdrawn by the applicant itself, thereby demonstrating that the BNB/ECB can employ other means that are effectively a barrier to entry.

567. Other financial licensing authorities' checks are conducted to a certain extent through open-source information and by accessing the Unified Citizens Register to identify family members of an applicant who could then be checked using the criminal convictions database maintained by the MoJ.

[57] Notaries are required to re-apply for registration annually and number around 700.

Ongoing monitoring for compliance with the licensing requirements

568. There are no separate processes established by the licencing authorities to check the compliance with the licensing requirements and fitness and propriety of the existing licensees on an ongoing basis, except for notaries[58]. Financial supervisors report that checks on licensing are conducted as part of their supervision activities (e.g., during onsite examinations).

569. The BNB reported that it conducts annual source of funds and source of wealth checks of existing shareholders with holding in excess of 3 per cent; and re-checks public domain information annually as part of the risk-assessment process and as part of the onsite inspection process. Similarly, the FSC claims that additional licensing related checks forms part of on-site examinations.

Detection of unlicensed businesses

570. Proactive measures to identify the activities without a licence or registration are conducted by the BNB and the FSC to some extent. In order to establish whether any persons are conducting licensable activity, the authorities primarily focus on checking the activities of entities that have been identified through checks of the company registration information[59] or that are reported to them by the other agencies and/or through customer complaints.

571. The BNB reported some instances of unregulated PI and EMI activities being identified through consumer complaints. From 2016-2021, the BNB initiated 30 inspections of entities suspected of carrying out unlicensed MVTS. In the majority of cases, the inspection could not be completed as activities are not being carried out from the entity's official address, therefore communication cannot be established. Therefore, only few cases are subject to regulatory or criminal sanction. In 2018, the BNB issued a BGN 15 000 (approx. EUR 7 500) sanction against an entity for conducting banking activities (lending to natural persons and attracting deposits) without the necessary licence. Despite the fact that OEs met onsite were admitting the fact of (potential) presence of hawaladars in Bulgaria, as well as the FID-SANS, the BNB was unaware of any such instances of hawala banking as LEAs do not officially notify the BNB in this regard. This proves cooperation gaps between authorities and limits the authorities' ability to allocate targeted measures to prevent unlicensed businesses from operating.

572. The FSC maintains a list of websites operated by the unlicensed online investment service providers (identified through customer complaints[60]) and shares this list on the FSC website. If the unregulated service continues three days following publication on the FSC's website, the FSC shall submit a request to the Chairman of Sofia District Court to order all enterprises providing public electronic communications networks and/or services to suspend access to these websites. The AT was advised of instances where website access from Bulgaria has not yet been suspended which suggests that the orders of the Court are not always complied with. As with suspected

[58] Criminal convictions of the notaries immediately result in deregistration by the MoJ. Within the reporting period, 1 notary had their registration withdrawn due to disqualification (which includes due to criminal offence) or incompatibility (conflicts of interest) and 2 due to disciplinary sanctions imposed.

[59] Checks are carried out on entities with company name or noted activities that appear to be licensable (e.g., those with the term "bank" in their name).

[60] A total of 416 complaints have been received against companies operating without licence during the period 2017-2021. The most prevalent typologies relate to client fraud cases, where potential clients receive phone-calls from a "consultant" claiming to represent a certain platform/investment company with an offer to invest in CFD/cryptocurrencies/shares, etc., however, when the victim attempts to withdrawn invested funds, communication is disrupted.

unlicensed MVTS, the activities tend not to be conducted at the official address, therefore communication is not possible.

573. The NaRA carries out checks against the Commercial Register to identify entities that appear to be offering VASP services and invites them to register. No measures are reported by other licensing/registration authorities to detect unlicensed business operations.

6.1.2. Supervisors' understanding and identification of ML/TF risks

574. Overall, supervisors' identification and understanding of ML/TF risks is varied. Understanding is reasonable regarding ML risks for financial institutions licenced by the BNB and the FSC, however, risk methodologies and their application methods lack clarity, are inconsistent and include duplication of efforts. Risk understanding by the CRC and the NRA require fundamental improvement and FID-SANS understanding of DNFBP sector risks, which is hampered by lack of available data, needs to be developed. In all cases, TF risk understanding is less developed than that of ML risk. This might be largely explained by the absence of TF-risk related data points in the supervisory data returns from the OEs. Similarly, supervisors do not collect any data to form their understanding on TFS related risks and controls.

575. The BNB, the FSC and the FID-SANS demonstrate fair understanding of the broader ML risks present in the financial sectors, however, the depth of institutional risk understanding is hampered by the shortcomings in the risk assessment processes (detailed analysis of risk assessment processes of each supervisory authority is presented in the below sections).

576. Understanding of ML risks by the FID-SANS[61] is developed to a lesser degree for the DNFBP sectors than for the financial sector. This might be attributed to the lack of risk data collection from the individual DNFBPs as well as regulatory gaps, e.g., absence of market entry measures for some sectors.

577. The FID-SANS, the BNB and the FSC routinely collect data for risk-assessment purposes regarding banks, EMIs, PIs and entities operating in securities and insurance sectors. The banks and PI/EMIs are approached by both, the BNB and FID-SANS; and securities and insurance - by the FSC. The data points collected by different supervisors for risk assessment purposes are similar but not entirely aligned, creating duplication of effort for OEs and neither supervisor having access to all data from both sets of questionnaires. In some cases, the results of the FID-SANS and the other supervisors' risk-assessments vary, however, (joint) supervisory programmes (see risk-based supervision) are determined on basis of meetings and dialogue between the supervisors rather than on the ratings alone. In all cases, risk assessment is carried out manually without the use of specialised software. Throughout the evaluation process the AT has, on various occasions, been presented with inconsistent, missing and contradictory data. One notable example is the inconsistent categorisation and count of OEs. This calls into question the supervisors' ability to access, analyse and rely upon data for risk assessment purposes. A lack of automated IT systems and reliance on manual systems is considered to be a contributing factor.

[61] FID-SANS is the legally appointed AML/CFT supervisor for all types of OE. It carries out its supervisory duties with cooperation of other supervisory authorities, identified in the LMML/LMFT – the BNB (for banks, EMIs and PIs), the FSC (for insurance and securities sector) as well as with the NaRA (for gambling operators, currency exchangers) and the CRC (for PMOs). The legal basis for AML/CFT supervision by the NaRA regarding currency exchange and the CRC regarding PMOs is not clearly established, see R.27.

FID-SANS

578. The FID-SANS' ML/TF risk understanding derives to large extent from the NRA and the NRA WG of which the Chairperson of SANS is the co-chair; and to some extent is informed by offsite (data returns) and onsite supervision. Although the FID-SANS demonstrates knowledge of broader risks, it has limited understanding of threats and vulnerabilities in the supervised sectors and different types of institutions and could not articulate how the risks can manifest.

579. Since 2018, the FID-SANS requires annual data returns[62] for risk-assessment purposes of banks, EMIs/PIs and other FIs under LCI. Returns were also obtained from insurers since 2018, however, they were temporarily ceased in 2020 before being reinstated in 2021. The AT was advised that they were ceased due to the NRA identifying the sector as low risk prior to the FID-SANS' own risk assessment of 2020 where FID-SANS established that only 2 of 13 were low risk (see table 6.1). This demonstrates somewhat contradictory findings between the NRA and the FID-SANS' risk assessment. No offsite analysis or risk assessment has been carried out for individual DNFBPs, VASPs or PMOs. The lack of risk assessment for these sectors is of a particular concern for PMOs (due to money remittance transfers), real estate (due to the risks identified in the NRA) as well as for VASPS, currency exchange and DNFBPs for which the FID-SANS is the sole supervisor; more detail is provided at section 6.1.3. on supervision.

580. For the sectors that are surveyed by the FID-SANS periodically, the risk assessment is formed on the basis of inherent risk data and controls. Questions include: (i) size (incl. offices, agents) of the entity and ownership and management structure; (ii) number and value of various products offered; (iii) customers (including number of natural persons, legal persons, foreign persons, high risk customers, PEPs); (iv) AML/CFT function within the entity; assessment of AML/CFT risks and internal AML/CFT rules; (vi) in addition, for banks, EMIs and PMOs, incoming and outgoing transactions with country breakdown.

581. Although the set of data points is reasonable and data was utilised for NRA purposes, the authorities were unable to confirm to what extent all of the above information is used to inform FID-SANS' risk understanding about banks, securities and MVTS. For example, there is no evidence provided that the authorities make use of wire transfers information in their supervisory assessments systemically, as the AT was not provided with the consolidated statistics of wire transfers broken down by geographies except in relation to the 2019 NRA exercise. Geographical breakdown of wire transfers data is not shared with the BNB or the CRC as this is not included in their own risk data analysis.

582. According to the FID-SANS risk assessment methodology, OEs are risk rated as Low, Medium or High. However, statistics provided do not evidence that risk assessments have been carried out by the FID-SANS in accordance with current methodology for the following reasons: (1) Not all financial institutions under LCI were included in statistics[63]; (2) Statistics provided to AT are based on 5 risk categories (Low, Low to Medium, Medium, Medium to High, High)[64]; (3)

[62] Sectors that are risk assessed by the FID-SANS on the basis of annual returns remains unconfirmed; as well as related statistics in table 6.1.

[63] This is due to certain entities being generally assessed as lower risk and excluded from detailed analysis including FIs that carry out guarantee transactions, money brokerage, factoring, forfeiting and acquisition of holdings in credit institution or other FI.

[64] Authorities explained that the 3-level approach resulted in vast majority of entities being categorised as 'Medium' so further categories were added although there was no established methodology for this at the time of the onsite.

No statistics provided for PIs, EMIs or investment linked pension insurance; (4) Although authorities reported that information for risk assessment purposes is being collected also from PMOs, currency exchangers, no evidence has been established that such risk assessments are conducted in practice.

Table 6.1. FID-SANS AML/CFT risk assessment, 2020

	Low	Medium to Low	Medium	Medium to High	High	Total
Banks	5	6	10	3	1	25
Financial institutions	1	66	36	2	0	105
Life insurance	2	2	3	6	0	13

Bulgarian National Bank

583. The BNB demonstrates fair understanding of the ML risks (the BNB was significant contributor to NRA) in the banking sector, however, MVTS (PI/EMIs) risk exposure is somewhat underappreciated. The depth of risk understanding largely correlates with the thoroughness of the risk assessment processes. Authorities consider the approach taken for PI/EMI is proportionate to the activities conducted whereas AT considers this needs to be enhanced as detailed below.

584. Throughout the reporting period, the BNB has routinely collected risk assessment data via a semi-annual questionnaire to banks and an annual questionnaire to payment service providers (covering both PIs and EMIs). Other FIs are supervised for AML/CFT by the FID-SANS.

585. Although both types of data returns include information on some types of inherent risks, as well as elements of internal controls, the scope of data set needs nevertheless be expanded. Neither questionnaire seeks volume and value of transactions by country although the payment service provider questionnaire does include breakdown by domestic, EU country, third country and high risk third country. However, the BNB advises that such granular information (with country breakdown) is collected from banks as part of supervision process but not currently as part of the risk data returns. The BNB advised that banks, PIs and EMIs will be required to provide more granular breakdown of payments by geography on a quarterly basis from Q2 2022 in accordance with ECB regulations. The questionnaires would also benefit from more granular detail on the main business lines of the bank (products and services), transactional and operational activities of the clients (broken down by client grouping), as well as delivery channels related data and statistics.

586. In addition to expanding the scope of data points collected for risk assessment purposes, the BNB risk assessment methodologies for banks also require further revision. The BNB risk assesses banks in two ways: (1) on an annual basis utilising data collected through the semi-annual questionnaires described above which primarily focus on inherent risks; and (2) on ad hoc basis as part of supervisory activities focusing on the controls applied in order to mitigate the inherent risks. Further enhancement would be beneficial regarding the precise calculation method of inherent risks as well as the correlation between inherent and residual risks and how a final or overall risk rating is produced.

587. In some cases, infractions identified by the BNB regarding banks appear (moderately) serious and similar infractions are identified in subsequent years which does not suggest that the offsite controls assessment process is very helpful integral part of the risk-based supervision that

consequently is expected to have an effect on the OEs' level of compliance. That is especially relevant in the area of TF risk understanding, which is underdeveloped by both the supervisory authorities and the OEs and consequently few mitigation measures are applied to prevent TF from occurring. Another important aspect is preventive measures in relation to TFS implementation and exposure to TFS evasion in general, that is not monitored offsite. For example, one bank met onsite has confirmed it did not have in place procedures regarding trade finance or dual use goods despite stating that it does have clients that are traders in such areas. Authorities advise that, due to only two TF risk events being raised in the NRA, less focus is given to TF supervision, however, sole reliance on past TF tendencies is not fully justified and can prevent the supervisory authorities from identifying current and emerging risk in a timely manner. On a positive note, the BNB reported that it is in the process of updating its risk assessment methodology for banks which will include further emphasis on inherent risk factors and greater clarity on the divide between inherent risks and quality of controls.

588. The BNB has been exercising AML/CFT control with regard to PIs and EMIs since March 2018. The first risk assessment exercise was conducted in 2019. The third risk assessment is due for completion by the end of Q1 2022[65]. Risk assessment of PI/EMIs takes into account inherent risk data factors with some consideration given to internal control mechanisms and results in 3 levels of risk categorization. Diverging methodologies describing the risk assessment process and the use of its results have been provided by the BNB; for example, the 2019 Handbook for Payment Supervision does not support that the onsite inspection plan for PI/EMIs is being determined on the ML/TF risks and sets out criteria that are not ML/TF risk related, such as market share; complaints; fraud data; significant or operational or security-related incidents, etc.

Table 6.2. BNB AML/CFT risk assessment –banks[66]

		2018	2019	2020
Banks	Low	2	1	0
	Moderate	16	16	15
	Elevated	0	1	3
	High	0	0	0
Branches of foreign banks	Low	3	3	3
	Moderate	1	1	2
	Elevated	1	1	2
	High	0	0	0

Table 6.3. BNB AML/CFT risk assessment –PI/EMI

		2019	2020
Payment institutions	Low	3	5
	Medium	1	0
	High	0	0
E-money institutions	Low	0	0
	Medium	3	4
	High	2	1

[65] 2022 risk assessment is to include information from PI/EMI institutions registered in other Member States and providing services in Bulgaria through its agents' branches.
[66] Whilst the overall numbers remain broadly the same, the rating of several individual banks has either decreased or increasing during 2018-2021.

Financial Supervision Commission

589. The FSC demonstrates fair understanding of the ML risks, being able to elaborate not only on the NRA findings (FSC was significant contributor to NRA), but also the most relevant risks to their regulated sectors, such as entities with high concentration of assets, geographical diversity, remote clients and clients that are subject to the residency investment scheme. The representatives also described measures taken to address the risks identified, such as targeted or thematic inspections.

590. In order to risk assess the securities and insurance sectors, the FSC collects the data on an annual basis. However, the scope of data sets needs to be expanded to better inform supervisory risk understanding, e.g., no analysis of financial flows is included. Shortcomings are also noted in risk calculation methodologies, see section 6.1.3 for more information. Whilst both inherent risk and risk mitigations are assessed for the securities sector, the latter is not considered for the insurance sector (both, insurance and investment linked pension insurance).

Table 6.4. FSC AML/CFT risk assessment, 2020

	Low	Medium to Low	Medium	Medium to High	High	Total
Insurance brokers	171	21	16	0	0	208
Life insurance	8	3	2	0	0	13
Non-bank investment intermediaries	0	0	22	16	0	38
Banks providing investment services	0	5	13	1	0	19
Management companies	0	13	16	2	0	31

National Revenue Agency

591. The NaRA participated in the NRA process in its general capacity and as the licensing authority for currency exchange offices. The NaRA did not contribute to the NRA regarding gambling entities or VASPs as the NRA was conducted prior to the NaRA's remit being expanded to include supervision of gambling operators and registration of VASPs. Partly due to the fact that changes affecting the scope of NaRA supervision are very recent and partly due to a lack of offsite monitoring processes, the NaRA could not demonstrate understanding of the ML/TF risks in its supervised sectors. During the onsite meetings, the NaRA representatives seemed to downplay the risks present in the currency exchange sector, commenting that there had been no indications of ML/TF risk to date. This view is not aligned with the conclusions of the NRA and does not take into account the issues of non-compliance with AML/CFT requirements by the sector.

592. No routine collection of data for AML/CFT risk-assessment purposes had been established for any sector[67] supervised by the NaRA. Currency exchange offices are risk-assessed to some extent based on transactional values (incl. negative information on licensees), however, this does not constitute an effective AML/CFT risk assessment. Supervisory data and information used by the former gambling supervisor, the SCG, was not made available to the NaRA. Absence of risk assessment for AML/CFT purposes limits the understanding by the NaRA on the risks to which its supervised sectors are exposed. However, on a positive note, the NaRA (in cooperation

[67] For two years, the NaRA has had access to the real time transactions performed by bureaux de change (volumes and size of transactions). Prior to this, daily reports were submitted to the NaRA. However, this data is obtained for fiscal purposes.

with the FID-SANS) is in the process of developing risk assessment tools for all supervised sectors, including gaining real-time access to online gambling servers.

Communications Regulation Commission

593. The CRC representatives were unable to confirm any involvement in the NRA process, could not demonstrate any ML/TF risk understanding. It was explained that, to date, supervision had not been risk-based and no ML/TF risk assessment of PMOs had been conducted by the CRC[68]. It was apparent that the CRC did not have the necessary resource or expertise to conduct effective AML/CFT supervision; moreover, the CRC does not have clear legal basis to conduct ML/TF supervision, especially with regards to applying sanctions for AML/CFT breaches. There is very little proactive cooperation and communication with the FID-SANS which is the main supervisory body for PMO supervision. This hampers the identification of risks in the PMO sector and does not allow for targeted risk mitigation.

6.1.3. Risk-based supervision of compliance with AML/CFT requirements

Summary conclusions and common findings

594. Overall, risk-based supervision of compliance with AML/CFT requirements is achieved to some extent regarding entities licensed by the BNB and the FSC. Supervision of the DNFBPs sector require fundamental improvements. The different supervisors have varying powers, resulting in duplication of efforts. In general, there is a lack of identification of serious breaches and breaches relating to TFS. Some sectors are subjected to very few inspections, especially DNFBPs including the most material ones, such as real estate, lawyers, accountants, etc. Supervision of the gambling and VASP sectors require significant development.

595. *AML/CFT supervision*. Supervisory arrangements in Bulgaria are rather complex. The LMML and LMFT establish that on-site inspections may be conducted independently by the FID-SANS or jointly with the other supervisors, namely the BNB (regarding banks, PIs and EMIs), the FSC (regarding securities, life insurance and pension insurance) and the NaRA (regarding gambling operators). Furthermore, the law establishes that supervision may be conducted by other supervisors that are not specifically named, hence the questionable legal basis for AML/CFT supervision carried out in practice by the NaRA (regarding currency exchange) and the CRC (regarding PMO); see R.27 for more information. This misalignment could be a barrier to successful application of regulatory or criminal sanctions for non-compliance identified during such supervisory activities. Only the FID-SANS has the remit to supervise ML suspicious transaction reporting. No such barrier appears to exist regarding supervision of suspicious transaction reporting on TF, however, authorities did not make this distinction.

596. *TFS supervision.* The BNB, the FSC and the NaRA have the powers to supervise compliance with the TF-related TFS requirements by the banks, EMIs, PIs, securities, insurance and gambling; the rest of the entities fall under the scope of TFS related to TF supervision under the FID-SANS. There are no offsite tools to supervise compliance by the OEs with TFS related to TF and/or OEs risk exposure in this area. However, all supervisory authorities uniformly stated that they include TFS element as part of full scope AML/CFT examinations. No sanctions have been applied for TFS

[68] Although statistics are collected routinely for the CRC's annual report, the information is not used for risk-assessment purposes and does not include statistics regarding the source or destination country of cross-border orders despite such information being held by the FID-SANS.

related to TF breaches to date, as all supervisors were claiming that no severe breaches have been identified to date which seems unusual due to the TFS-related deficiencies by the OEs identified by the AT, see IO4.

597. Although the FID-SANS, the BNB and the FSC demonstrated fair knowledge of AML/CFT supervision, the effectiveness of the supervision is hampered by the shortage of resources, incl. human, financial and technical, especially in FID-SANS. Other supervisory authorities, in addition to the urgent need to increase resources, also need to deepen their expertise in AML/CFT supervisory matters. The governance issues concerning the FID-SANS, and the former gambling supervisor has negative implications on the continuity of supervisory plans, retaining expertise and overall supervisory effectiveness.

Financial sector supervision: summary conclusions and common findings

598. Duplication of supervision in some cases creates unnecessary strain on resource to both supervisors and the OEs; which, combined with the lack of clearly defined risk-based joint supervisory methodologies, makes it harder to achieve efficiency and effectiveness of the joint supervisory actions. In some cases, both offsite and onsite supervisory activities are duplicated; OEs are required to submit similar statistical returns to both the FID-SANS and some other supervisors the results of which often vary in practice. Linked to this, some entities receive multiple on-site inspections within a short timeframe. Authorities reported that draft annual supervisory plans are decided upon as result of exchange of information and meetings between the authorities and that, in cases of divergent views, a conservative approach would be taken and the higher rating would be applied.

599. Overall, the supervision of core principles FIs and PIs/EMIs carried out by the FID-SANS, the BNB and the FSC cannot be considered fully risk-based. Although supervisors have established methodologies that to some extent explain how the risk profiles of the supervised individual institutions drive the frequency and intensity of the future supervisory actions, the practical arrangements suggest otherwise. Except for the banking sector, the planning of the onsite examinations does not seem to be fully risk-driven; and supervisory measures are mostly limited to onsite examinations, with no consideration given to other forms of supervisory engagement in accordance with risk. In addition, the quality (the depth) of the onsite examinations needs to be further increased[69], in particular concerning (1) sample testing of client files; (2) conclusions on the breaches of the AML/CFT requirements in the onsite inspection reports which are not always firm or explicitly stated; (3) linked to this, content of the onsite inspection reports hardly suggest whether AML/CFT breaches were serious (if so, what is the level of seriousness), repeated and/or systemic nature. The AT found that the serious shortcomings are not treated as serious enough by some supervisors.

DNFBP sector supervision: summary conclusions and common findings

600. The effectiveness of the DNFBP supervision cannot be demonstrated. AT expresses serious concerns on limited capability of the FID-SANS to conduct effective supervision of the lawyers, accountants and persons that conduct TCSP activities due to the following: (a) no data is available on how many lawyers and accountants established in Bulgaria conduct FATF covered activities; (b) no data is available how many accountants and lawyers act as TCSPs, nor there is a separate licensing regime established for the TCSPs; (c) accountants are not subject to market

[69]Based on the sample of the onsite examination reports shared with the AT by some supervisory authorities

entry measures thus the population is not determined; (d) no periodic data returns are being collected from lawyers and accountants enabling the supervisors to assess the risks present in these sectors and risk exposure of individual entities, incl. sole practitioners. This does not allow for efficient use of resources that needs to be allocated in accordance with risks thus creating the potential that highest risk presenting entities are left outside the scope of onsite supervisory checks. The number of accountants and lawyers subjected to onsite examinations is extremely low. Although certain professional and self-regulatory bodies (e.g., lawyers, accountants) do, to some extent, conduct checks that AML/CFT policies and procedures are in place as part of their general oversight, there is no legal basis neither for this, nor for sanctioning for AML/CFT breaches, therefore they are not considered AML/CFT supervisors for the purposes of the MER. Supervisory attention to real estate and VASPs sector is also not sufficient, especially given their high exposure to risks.

601. The supervision by the NaRA and the CRC is not risk-based. In general, these supervisors are ineffective in carrying out the supervisory duties and little evidence and statistical data was provided to the AT to prove otherwise.

FID-SANS

602. The FID-SANS is a proactive supervisor, however, its efforts to achieve greater supervisory effectiveness are hampered by the significant lack of resources, i.e., insufficient number of staff and the absence IT tools to assist in carrying out daily supervisory tasks. FID-SANS reported that following the restructuring of the FID-SANS in January 2021, the number of staff has increased, however, the actual numbers have not been disclosed, nor was there an organigram of an organization chat presented to the AT upon request. Based on the relatively low numbers of inspections[70] (especially regarding DNFBPs that are not subject to supervision by other authorities), it cannot be established that the FID-SANS has the necessary resource to supervise AML/CFT effectively.

603. Supervisory processes designed by the FID-SANS are risk-based only to some extent. Although data gathered for offsite monitoring purposes to some extent informs the FID-SANS' judgement on the onsite examinations of the financial sector (banks, EMIs, PIs, securities and insurance), no such data is gathered from the DNFBPs, thus supervisory measures planning for the DNFBPs sector is not risk-based to more than a minor extent. At the time of the onsite, measures were under development although efforts were impeded by lack of available data on entities that conduct activities covered by the FATF Standard (especially concerning legal and accountancy sectors).

604. Risk assessment processes and planning methodologies regarding supervisory actions are rather chaotic, do not always link together and the processes described in the regulatory documents do not always correspond with the practical arrangements. Since 2019, the FID-SANS utilizes 5 levels of risk (see statistics provided in tables 6.1 and 6.5) whereas the internal process documents refer to a 3-risk rating approach where high risk entities are usually subjected to onsite examinations, medium risk – to remote checks on internal AML/CFT procedures and low risk are not subject to any measures unless trigger events occur. The AT was advised that the 3-level risk assessment process was flawed as it resulted in the vast majority of entities receiving

[70] Number of onsite examinations has further reduced in recent years as evidenced by statistical data.

'Moderate' risk rating and so this category was split into three which along with the Low and High categories equates to the 5-risk level approach that is followed in practice. No methodology was available to describe how the 5 risk level assessments are carried out or how this impacts upon supervisory activities. Therefore, there is inconsistency between the (flawed) documented procedures and what happens in practice and statistics are also inconsistent or unreliable.

605. No distinction is made between financial institutions other than banks and insurance in the FID-SANS risk calculation which does not support that a risk-based approach is followed. Moreover, it is not clear how the risk rating drives the frequency of the onsite examinations in practice, e.g., the below data shows that 40 % of *medium* risk banks have been subjected to onsite examinations, whereas from *medium to low-risk* category - 50%. This does not seem to be supported on the basis of risk, neither aligned with the supervisory methodologies used. No distinction is made by the FID-SANS in terms of scope (intensity) of the supervisory actions in accordance with the individual risk profiles.

Table 6.5. FID-SANS supervision by risk category, financial institutions, 2020

	Low	Medium to Low	Medium	Medium to High	High	Total
Banks	5	6	10	3	1	25
Onsite examinations	1	3	4	2	1	11
Other supervisory actions	0	0	0	0	0	0
Jointly with BNB	1	3	3	1	1	9
Financial institutions	1	66	36	2	0	105
Onsite examinations	0	1	7	1	0	9
Other supervisory actions	0	0	0	0	0	0
Joint examinations	0	0	0	0	0	0
Life insurance	2	2	3	6	0	13
Onsite examinations	0	0	0	0	0	0
Other supervisory actions	0	0	0	0	0	0
Joint examinations	0	0	0	0	0	0

606. Remote checks of internal AML/CFT policies. Prior to the 2019 amendments made to LMML, OEs were obliged to submit internal AML/CFT rules to FID-SANS for approval. During 2015-2019, FID-SANS processed a total 6 586 draft rules and issued a total 1 442 instructions to eliminate non-conformities. Since then, the FID-SANS has continued such checks under a risk-based approach, 45 of which were conducted in 2021. Such checks were carried out for all new VASPs and PMOs.

607. Onsite visits: financial sector (see table 6.6). The total number of financial sector onsite inspections carried out by the FID-SANS is extremely low, except for banks. That might be attributed to limited capacity of the FID-SANS to fully implement supervisory action plans for the financial sector, for example, planned inspections of life insurance sector have not been carried out in 2020 despite there being 6 entities assessed as *medium to high* risk, which should have received supervisory attention.

608. Onsite visits: DNFBP sector (see table 6.7). The total number of DNFBP onsite inspections carried out by the FID-SANS is extremely low; there are periods when certain sectors are left without any supervisory attention. The authorities advise that this was due to both focusing staff to the NRA and due to the Covid-19 pandemic. It is evident that the FID-SANS does not take into account the risk exposure of the different DNFBP sectors and individual entities. For example, during reporting period only 9 inspections were carried out for real estate agents which are rated as high risk in NRA; no supervisory measures (be it remote or onsite) of gambling operators have

been carried out by the FID-SANS since 2019 despite allegations of corruption against the former Chairperson of the SGC that resulted in its dissolution.

609. Based on the findings of onsite examinations, the FID-SANS publishes annual reports that include an overview of the most common types of deficiencies identified. The entities with the widest range of infractions identified during the reporting period are banks. In some cases, infractions appear (moderately) serious and similar infractions are identified in subsequent years, thus are repeated in a general sense[71]. Another notable example mentioning is currency exchange providers that have relatively serious infractions, such as failing to conduct CDD on clients, notify the FID-SANS of suspicion and large cash transactions over EUR 15 000 and even not having AML/CFT procedures in place. This is despite statistics stating that currency exchange inspections were only conducted by the FID-SANS in 2016 (see table 6.6.). In general, commonly identified breaches found by the FID-SANS during onsite examinations are not fully commensurate with the risk exposure of the entities, especially given the context of the country and possible implementation gaps discussed under IO.4.

610. The FID-SANS, as the only supervisor having powers to examine compliance by the OEs with the STR reporting requirements, has identified only 31 instances of non-reporting during 2015-2020 which seems at odds given the monitoring related shortcomings by the majority of OEs that subsequently give raise to an STR, as discussed under IO.4.

611. Given the low amount of supervisory engagement with almost all sectors, except banks, effectiveness of supervision needs to be significantly enhanced.

Table 6.6. FID-SANS Inspections - Financial Institutions

	2015	2016	2017	2018	2019	2020	As at 31.07.21	TOTAL
Banks	28	27	27	26	25	25	25	-
Onsite inspections	12	7	8	2	7	11	2	49
Securities								
Investment Intermediaries	70	65	64	60	60	56	56	-
Onsite inspections	10	8	2	0	1	0	2	23
Management companies	31	31	31	31	31	30	30	-
Onsite inspections	2	3	1	0	0	0	2	8
Insurance								
Life insurance	13	12	12	11	11	10	10	-
Onsite inspections	0	2	0	0	3	2	0	7
General insurance	29	26	26	N/A	N/A	N/A	N/A	-

[71] "Repeated" has particular meaning in LMML of being a breach identified within one year of imposition of sanction for same type of violation.

Onsite inspections	3	0	0	0	0	0	0	3
Insurance brokers	398	394	385	263	249	218	208	-
Onsite inspections	2	1	0	0	0	0	0	3
Agents	20 983	19 249	12 239	8 427	3 253	2 992	3 334	-
Onsite inspections	0	0	0	0	0	0	0	0
Pension insurance	9	9	9	9	9	9	9	-
Onsite inspections	2	1	0	0	0	0	0	3
MVTS								
Exchange merchants[72]	760	556	814	815	810	786	944	-
Onsite inspections	0	20	0	0	0	0	0	20
Postal Money operators	17	18	23	25	29	38	37	-
Onsite inspections	1	0	1	0	0	0	7	9
E-money since 2018	-	-	-	5	5	6	8	-
Onsite inspections	-	-	-	1	2	2	1	6
Other FIs								
Financial institutions (under LCI)	170	180	190	190	198	213	203	-
Onsite inspections	1	6	5	1	5	10	8	36
Leasing	2449	2630	2825	2952	3028	3076	-	-
Onsite inspections	1	1	2	0	0	0	1[73]	5

Table 6.7. FID-SANS Inspections - DNFBPs

	2015	**2016**	**2017**	**2018**	**2019**	**2020**	**As at 31.07.21**	**TOTAL**
Gambling								
Gambling halls	738	786	867	894	942	N/a[74]	1 047	-
Onsite inspections	0	0	0	0	0	0	0	0

[72] AT was advised that this includes money transmission, however, statistics shows that this is not the case, i.e., number of entities is too low.
[73]This inspection is off-site, not on-site.
[74] Precise number of entities is not available due to closing of the former regulator, the SCG

Casinos (incl remote casinos until 2020)	25	27	25	23	22	23	20	-
Onsite inspections	4	3	5	7	0	0	0	19
Remote casinos	-	-	-	-	-	7	7	-
Off-site checks	-	-	-	-	-	0	4	0
Estate agents	2 469	2 630	2 544	2 540	2 779	2 724	N/a[75]	-
Onsite inspections	2	0	4	0	0	0	3	9
Lawyers	13 013	13 500	13 720	13 640	13 825	13 994	13605	-
Onsite inspections	7	12	1	0	0	0	5	25
Notaries	645	666	675	672	730	723	719	-
Onsite inspections	12	1	10	6	0	0	0	29
Accountants	10 654	11 604	12 067	12 703	13 048	12 842	TBC	-
Onsite inspections	8	4	7	0	1	5	0	25
Auditors	704	722	716	706	710	702	696	-
Onsite inspections	1	7	1	0	0	0	0	9

Bulgarian National Bank

612. AML/CFT supervision of banks is conducted by the AML/CFT department (consisting of 12 members of staff) of the BNB-SSAD. AML/CFT supervision of EMIs and PIs is conducted by the Bulgarian National Bank Specific Oversight of Payment Services Division of the Methodology and Financial Markets Directorate (BNB-MFM) within the Banking Department (consisting of 6 members of staff). This unit is not only tasked with the AML/CFT supervision of PIs and EMIs, but also licensing. The split of the AML/CFT supervisory duties between two departments does not lead to efficient use of resources and supervisory tools, although number of staff seems to be commensurate with the size of the supervised sectors. This may also hamper the understanding of the risks by the BNB in the MVTS sector.

613. The BNB conducts supervision of entities using a combination of onsite and offsite measures. Frequency and scope of the onsite inspections are decided upon risk categorisation. Onsite supervision may be conducted solely by the BNB or jointly with the FID-SANS and can be either full-scope or targeted. The risk category of the individual entities also informs the length (in terms of time spent onsite) and depth of onsite examinations[76]. Following the recent changes to the risk based supervisory approaches, only thematic or targeted examinations have been carried out since 2020, e.g., 8 joint inspections with FID-SANS (covering CDD, beneficial ownership, PEPs, simplified and enhanced CDD, monitoring of customers, source of funds and the

[75] Figure is not available.
[76] e.g., low risk takes 2 staff up to 15 days, moderate takes 2-3 staff up to 20 days, elevated risk takes 2-3 staff up to 25 days, high risk takes 3 staff up to 30 days.

internal AML/CFT unit of banks); 1 individual AML/CFT inspection covering 4 areas (risk assessment and internal rules, CDD measures, AML/CFT systems and reporting, AML/CFT unit and training); 1 individual targeted inspections covering compliance with LMML and RILMML regarding one particular client. Themes of the on-site examinations prior to 2020 (after this date findings of NRA were considered) do not seem to fully take into account the risks present in the country and in the sectors given the nature of products and services offered by the banking sector although some inspections did focus on particular themes such as private banking and cash transactions.

614. Number of inspections[77] for PI/EMIs is low but is increasing since BNB supervision commenced[78] (see table 6.9). In late 2020, the BNB commenced full scope AML/CFT inspections on all eight PI and EMIs licensed in other Member States that operate in Bulgaria through branches and agents due to identification of risks associated with cross-border business. Although banks receive more supervisory attention in terms of onsite checks, the total number of examinations is still not sufficient. Other supervisory measures allocated for the banking sector include review of the AML/CFT policies. However, the method used to allocate banks that are subject to offsite review of internal policies, is not established.

615. Commonly identified AML/CFT breaches in the banking sector include verification of clients and beneficial owners, establishment of the source of funds, enhanced CDD and measures applied to PEPs. Whilst EMIs commonly breach client identification requirements, followed by deficient client and business risk assessment, no shortcomings have been identified during the three inspections of PIs. The commonly identified breaches found by the BNB during onsite examinations are not commensurate with the risk exposure of the entities, especially given the context of the country and possible implementation gaps discussed under IO4[79] upon meeting with the private sector. The relatively low number of infringements in ML/TF monitoring area in the banking sector and zero infringements in PI/EMIs sector cannot be fully justified given the findings of the AT under IO4, that despite banks utilising sophisticated software and filing more STRs than other sectors, there seemed to be limited knowledge by the OEs on what to look out for to identify suspicion as well as deficient internal AML/CFT procedures in this regard, especially related to TF recognition and gaps in risk understanding (other shortcomings by OEs identified at IO4 include TFS related to TF implementation, PEP-related procedures, risk understanding, etc.) .

616. Onsite examination reports would benefit from greater clarity regarding conclusions on the breaches of the AML/CFT requirements in the onsite inspection reports which are not always firm or explicitly stated[80]; and, linked to this, content of the onsite inspection reports hardly suggest whether AML/CFT breaches were serious (if so, what is the level of seriousness),

[77] EMIs/PIs are subjected to only full scope onsite examinations; this sector become subject to BNB supervision in 2018.
[78] Regarding PI/EMI, full-scope onsite inspections were conducted during 2020 of 2 EMIs assessed as *High* risk in the 2019 risk assessment and during 2021, 1 onsite inspection was carried out of an EMI assessed as *Medium* risk in the 2020 risk assessment.
[79] This includes seemingly low number of clients identified as PEPs or high risk, and STRs (other than banks, PI and EMIs) and some FIs unable to articulate sound economic rationale for prevalence of large cash transactions as well as specific shortcomings noted regarding individual OEs.
[80] In addition to the inspection reports, the BNB also makes a report to the Deputy Governor that describes the type of violation and whether it is serious or repeated including proposal regarding penalties.

repeated and/or systemic nature. Instances were noted where the BNB described infractions as being minor or moderate, whereas the AT considered them to be more serious.

Table 6.8. BNB Supervisory measures according to bank risk category

	2015[81]	2016	2017	2018	2019	2020	As at 31.07.21	TOTAL
High - No. of banks	0	0	0	0	0	0	0	-
High - No. of inspections	0	0	0	0	0	0	0	0
Elevated- No. of banks	0	4	2	2	0	2	5	-
Elevated- No. of inspections	0	0	4	2	2	0	1	9
Moderate- No. of banks	25	6	6	18	22	17	17	-
Moderate- No. of inspections	10	11	2	4	8	9	6	50
Low- No. of banks	3	17	19	6	2	4	3	-
Low - No. of inspections	0	0	0	0	0	0	1	1

Table 6.9. BNB Inspections

		2015	2016	2017	2018	2019	2020	As at 31.07.21	TOTAL
Banks	Entities	28	27	27	26	25	25	25	-
	On-site inspections - Sole	7	9	7	7	9	2	6	47
	On-site inspections - Joint	3	2	0	0	1	9	1	16
Payment institutions	Entities	8	11	10	5	5	5	5	-
	On-site inspections - Sole	0	0	0	3	0	0	0	3
	On-site inspections - Joint	0	0	0	0	0	0	0	0
E-money institutions	Entities	2	3	3	5	5	6	8	-
	On-site inspections - Sole	0	0	0	1	1	0	1	3
	On-site inspections - Joint	0	0	0	1	0	2	0	1

Financial Supervision Commission

617. The FSC is organised into three principle divisions: Investment Activity Supervision, Insurance Supervision and Social Insurance Supervision. Following the NRA in 2020, an AML/CFT Unit was established within the Investment Activity Supervision Directorate to supervise the securities sector due to the NRA identifying higher risk in that area. The Unit cooperates and supports the other directorates regarding supervision of the other sectors. However, supervision of the insurance sector is split amongst other departments of the FSC and thus the total number of full-time employees dedicated for insurance supervision has not been established. The AML/CFT Unit currently comprises 6 members of staff and is supported in its work by other

[81] Inspections are based on the previous years' risk rating

departments that also carry out some AML/CFT supervisory duties. Although the FSC can be complimented for establishing the AML/CFT Unit, the efforts are very recent and therefore full effectiveness is yet to be seen. On a positive note, the staff met onsite demonstrated fair knowledge and motivation related to AML/CFT supervision. A permanent internal working group is operating within the FSC that is tasked with further enhancing a risk-based approach to supervision of securities and insurance sectors which is seen as additional strong element in further advancing supervisory practices.

618. The FSC's AML/CFT supervision of securities and insurance was not fully separated from the prudential supervision during the entire period under review, thus the intensity and frequency of the future supervisory actions were not fully driven by the ML/TF risks as opposed to prudential risk considerations. However, recent changes implemented since 2020 to the approach allows for supervisory actions planning based on ML/TF considerations to a larger extent.

619. Based on the risk assessment results, both, securities and insurance, entities are divided into 5 risk categories ranging from low to high. Risk categorisation is not used to inform the decision on carrying out onsite examinations to a full extent. The FSC reports that in addition to the results of risk assessment, previous onsite inspection findings, periodic compliance and prudential reports, incl. audit findings are taken into account when drafting onsite examination plan; however, the weight given to the risk assessments is not clearly defined. As a result, allocation of supervisory measures is not entirely risk based; for example, a relatively low percentage of entities that fall under medium risk category are subjected to onsite inspections which does not seem justified given that no entities fall under the high-risk category; moreover, some low-risk entities are subjected to onsite reviews which does not justify efficient use of resources and does not target the higher-risk entities. This can be partly attributed to shortcomings of the methodologies, especially in relation to approach to risk calculation and categorisation that are not always proportionate to the complexity of the different sectors. Improvements would allow not only for more targeted approach to risk monitoring and mitigation in the supervised sectors, but also - for more efficient use of limited supervisory resources.

620. In general, a low number of onsite examinations have been conducted by the FSC during the review period (recent increase is only noted in securities sector and only in the first half of 2021[82]). No supervisory measures apart from onsite examinations are allocated based on risk assessment results. This is concerning given the large number of entities that have not been inspected during the review period (see table 6.9).

621. The FSC reports that the most commonly observed infractions found during onsite examinations relate to identification of PEPs, application of enhanced CDD measures, verification of source of funds and CDD for non-face-to-face customers. The finding on remote CDD can be also supported by the AT findings (as discussed under IO4), where some FIs[83] pointed to fraud cases resulting from deficient remote identification practices. This calls for a need to strengthen the legal requirements for remote onboarding by introducing additional safeguards or

[82] In 2021, the newly established AML/CFT Unit performed 10 thematic inspections, 8 on investment firms (including one bank) and 3 on management companies. Four inspections were conducted jointly with FID-SANS; 2 on investment firms and 2 on management companies.

[83] These cases are mostly reported in the e-money and payment institutions, consumer lending and VASPS.

prohibiting some sectors to rely on remote identification practices partly (where some customers are prevented from onboarding remotely, e.g., legal persons) or fully; and consequently, taking sufficient actions to enforce these revised obligations. As for the other breaches commonly identified by the FSC, these can be expected given the shortcomings identified under IO4. However, zero infringements in the area of monitoring does not seem justified, especially given the findings of the AT under IO4 linked to limited knowledge demonstrated by the OEs on what to look out for to identify suspicion as well as deficient internal AML/CFT procedures in this regard, especially related to TF. The fact that monitoring is examined not only in full scope inspections, but also in thematic onsite examinations (suggesting that this area will be checked in more depth), is even more concerning.

622. Based on the above, the quality (the depth) of the onsite examinations needs to be further increased[84], in particular concerning (1) sample testing of client files; (2) conclusions on the breaches of the AML/CFT requirements in the onsite inspection reports which are not always firm or explicitly stated; (3) linked to this, content of the onsite inspection reports hardly suggest whether AML/CFT breaches were serious (if so, what is the level of seriousness), repeated and/or systemic nature.

Table 6.10. FSC supervisory measures according to risk category, 2020

	Low	Medium to Low	Medium	Medium to High	High	Total
Insurance brokers	171	21	16	0	0	208
Inspection	0	3	0	0	0	3
Life insurance	8	3	2	0	0	13
Inspection	2	0	2	0	0	4
Non-bank investment intermediaries	0	0	22	16	0	38
Inspection	0	0	4	9	0	13
Banks providing investment services	0	5	13	1	0	19
Inspection	0	0	2	1	0	3
Management companies	0	13	16	2	0	31
Inspection	0	0	4	1	0	5

Table 6.11. FSC Inspections

		2015	2016	2017	2018	2019	2020	As at 31.07.21	Total
Securities (investment firms)	Entities	42	41	41	38	38	36	36	-
	On-site inspections - Sole	1	1	1	1	1	4	10	19
	On-site inspections - Joint	0	0	0	0	0	0	2	2
Management companies	Entities	30	31	31	31	31	30	29	-
	On-site inspections - Sole	1	1	1	3	2	2	1	11

[84]Based on the sample of the onsite examination reports shared with the AT by some supervisory authorities.

	On-site inspections - Joint	0	0	0	0	0	0	2	2
Insurance	Life brokers& intermediaries General Insurance	339 390	220 369	217 369	263 N/A	249 N/A	218 N/A	208 N/A	-
	On-site inspections - Sole	3	0	2	4	1	0	2	12
	On-site inspections - Joint	0	0	0	0	0	0	0	0
Pension insurance	Entities	9	9	9	9	9	9	9	-
	On-site inspections - Sole	8	10	2	0	1	1	1	23
	On-site inspections - Joint	0	0	0	0	0	0	0	0

National Revenue Agency

623. The NaRA was not able to demonstrate that supervision of the casinos, incl. gambling operators with AML/CFT requirements is risk based and effective.

624. No documents on the organisational structure and little information on precise number of staff (except 5 employees responsible for gambling industry's supervision) tasked with AML/CFT supervisory duties was provided to the AT. The NaRA reported that the current organisational set up of the authority will be restructured and there are plans to retrain the existing staff to enable them to perform AML/CFT supervision.

625. Supervisory methodologies are currently under development. The NaRA advised that currency exchange offices are selected for AML/CFT inspection based on large transactions or issues of non-compliance with the tax legislation. No internal documents regarding inspection planning, scope, the results of inspections and related statistics were available.

626. No supervision, either remote or onsite, had been conducted by the NaRA over casinos and gambling operators. The NaRA was unable to provide any information or statistics regarding supervision conducted by the former supervisor, the SGC. Interviewed casinos advised they had no supervisory interactions with the former regulator.

Communications Regulation Commission

627. The CRC does not have a dedicated AML/CFT Unit. Staff members of the Control Directorate that are tasked with general supervision duties also conduct AML/CFT supervision as part of their general supervision processes. No organigram or information regarding the number of staff tasked with AML/CFT supervision was provided to the evaluators.

628. Supervision of the PMOs is not risk-based and not effective. AML/CFT supervisory actions by the CRC are limited to remote checks to ensure that written procedures are in place; this does not include any sample-checking. In 2020, 79 such checks were carried out with no deficiencies identified.

VASPS

629. The FID-SANS reported that AML/CFT supervision of VASPs started in 2021. At the time of the onsite, 9 had been inspected remotely with 3 reports still being finalised. The aim of the onsite supervision was to ensure that the newly registered VASPs had carried out risk assessments and had put in place internal procedures and controls for AML/CFT. The effectiveness of the supervision is hampered by the fact that the full population of VASPs is not known due to the deficiencies in the registration regime as well as the limited scope of the regulation concerning virtual asset-related activities that fall under the FATF standard (please see R.15, R.28 and section 5.1.1 above on licensing controls). No offsite reporting tools are in place to enable the supervisor to understand the risks to which the sector and individual VASPs are exposed.

6.1.4. Remedial actions and effective, proportionate, and dissuasive sanctions

630. Sanctions may be imposed against any type of obliged entity by the FID-SANS, the BNB (regarding banks, PIs and EMIs), the FSC (regarding securities and insurance) and the NaRA (regarding gambling operators). As for other sectors, the supervisors must notify the FID-SANS of infractions identified so that the FID-SANS may consider issuing a penalty. Conversely, the FID-SANS does not have the ability to impose regulatory sanctions such as revocation of a licence and must refer the case to the authorities that have issued a licence or registration. No data is available on sanctions imposed by the FID-SANS regarding violations identified by other supervisors, nor regulatory actions taken by other supervisors regarding violations identified by the FID-SANS.

631. Except for banks, PIs and EMIs, a low number of sanctions have been applied by the supervisory authorities to date and these are not considered dissuasive and proportionate; No sanctions have been issued to notaries and real estate agents to date. Supervisory authorities are not making use of the LMML provisions to issue more dissuasive sanctions, e.g., larger monetary fines for systemic and repeated violations (please see R.35 for more information), in cases when more serious or repeat breaches are identified. No sanctions have ever been applied to senior managers or directors to date. One reason cited for the lack of "serious and repeat" offences is that in order for a pecuniary sanction to be imposed for a repeated breach, it must take place within a year of the previous breach. Due to the time taken to plan, carry out and report on an inspection as well as given shortage of resources in some supervisory authorities, it is very unlikely for the supervisors to identify repeat breaches within 1 year.

632. The supervisory authorities have never issued sanctions for breaches of the LMFT legal requirements that related to TF prevention and TFS related to TF requirements. In light of limited TF risk understanding and TF-related TFS implementation shortcomings by the OEs, it is surprising that no serious deficiencies which would require remediation or sanctioning have been identified by the authorities concerning implementation of TF prevention measures.

633. FID-SANS typically imposes low value penalties in order to reduce, according to FID-SANS, the risk of court case and subsequent removal or reduction of a penalty which limits ability of the supervisor to issue proportionate and more dissuasive sanctions with a proven deterrent effect. However, since 2019 the FID-SANS publishes sanctions on its website, along with additional information on nature of the violation(s) and the name of the sanctioned entity, which adds a level of dissuasiveness to a sanction imposed.

634. The BNB mainly utilizes regulatory (i.e., remediation) measures[85], even in cases of repeated breaches claiming that no serious or systemic violations have ever been identified. The same applies to the FSC, although some low value fines have also been issued for the securities sector.

635. Interviews with banks and insurers met onsite suggest that opportunity is provided to the OEs to remediate identified AML/CFT breaches before it is determined whether a sanction should be applied. Because of this reason, two entities have reported that the onsite inspection report was issued nearly a year after the inspection, however, the authorities dispute this claim.

636. With the exception of the BNB regarding banks, none of the supervisory authorities have policies on the application of sanctions which might impact their ability to apply a consistent and proportionate approach towards sanctioning, i.e., determining the level of sanction(s) and/or value of monetary fines in accordance with the severity, repeated and systemic nature of breaches. The BNB Operational Rules include factors to consider when determining a sanction and the steps in the process but do not specifically state how to select a penalty or set the value of a financial penalty (or consider other sanctions) thus should be further revised and complemented to ensure practical applicability.

FID-SANS

637. Given the average amount of fines for an FI during the reporting period was c. EUR 1 700 for FIs and c. EUR 1 200 for DNFBPs, the sanctions cannot be considered proportionate and/or dissuasive. The AT was advised that the FID-SANS will typically apply the lowest possible sanctions due to past cases where financial penalties imposed by the FID-SANS were reduced by court judgement in cases where: (i) no previous infringements had been identified; (ii) the OE cooperated with the process; (iii) multiple infringements resulted in a larger penalties than each individual penalty would have been; and (iv) where, due to economic factors, the penalty was considered excessive. Of 192 appeals there were 9 instances of decrease in the penalty (in 2015 and 2016) and 40 instances of the penalty being revoked entirely (31 of which were in 2015 and 2016). In two cases in 2020, the penalty was reduced from BGN 20 000 to BGN 5 000 (approx. EUR 10 000 to EUR 2 500).

638. Although the average size of individual penalties amounts to only EUR 1 700 for FIs and EUR 1 200 for DNFBPs, there were a few cases in which larger penalties have been applied (comprised of multiple penalties issued for multiple violations). This relates to a case of a small bank with LMML violations whereby a bank was issued with multiple penalties, some of which for repeated breaches: BGN 65 000 (approx. EUR 32 500) in 2014, BGN 76 000 (approx. EUR 37 500) in 2015, BGN 5 000 (approx. EUR 2 500) in 2017 and BGN 20 000 (approx. EUR 10 000) in 2019. Such instances do not demonstrate that sanctions applied for systemic, severe and repeated deficiencies are proportionate and dissuasive.

[85] E.g., written warning, order to remediate deficiencies, etc.

Table 6.12. FID-SANS Sanctions – Financial institutions

		Banks	Securities	Insurance	Pension insurance	Other FIs[86]	E-money	Postal operators
2015	Written warning	1	0	0	0	0	0	0
	No. fines	21	3	9	4	2	0	1
	Value fines (EUR)	49 595	4 602	14 572	7 158	2 045	0	1 023
	Court cases	3	1	5	4	0	0	0
2016	Written warning	3	1	0	0	1	0	0
	No. fines	14	5	2	4	3	0	0
	Value fines	21 986	12 782	2 045	3 579	3 068	0	0
	Court cases	0	0	2	0	0	0	0
2017	Written warning	0	0	0	0	0	0	0
	No. fines	28	0	0	0	12	0	1
	Value fines	30 678	0	0	0	12 271	0	511
	Court cases	0	0	0	0	0	0	0
2018	Written warning	0	0	0	0	0	0	0
	No. fines	0	0	0	0	0	9	0
	Value fines	0	0	0	0	0	9 203	0
	Court cases	0	0	0	0	0	8	0
2019	Written warning	0	0	0	0	0	0	0
	No. fines	15	3	10	0	9	9	0
	Value fines	35 279	7 669	71 581	0	23 008	23 008	0
	Court cases	0	3	6	0	4	4	0
2020	Written warning	1	0	1	0	1	0	0
	No. fines	8	0	1	0	27	3	0
	Value fines	18 918	0	2 556	0	92 033	3 068	0
	Court cases	0	0	0	0	3	0	0
As at 31.07.21	Written warning	1	4	0	0	1	0	0
	No. fines	1	4	0	0	23	0	0
	Value fines	0	0	0	0	25 565	0	0
	Court cases	0	0	0	0	8[87]	0	0

Table 6.13. FID-SANS Sanctions – DNFBPs

		Gambling	Estate agents	Lawyers	Notaries	Accountants	Auditors
2015	Written warning	0	0	0	0	0	0
	No. fines	16	0	3	0	5	1
	Value fines (EUR)	25 565	0	4 602	0	5 119	250

[86]Statistics remain unconfirmed regarding MVTS and currency exchange.
[87] The rationale is unclear for 8 court cases relating to only 3 fines.

	Court cases	0	0	0	0	0	0
2016	Written warning	6	0	3	0	1	1
	No. fines	10	0	6	0	2	0
	Value fines	10 226	0	11 504	0	2 045	0
	Court cases	0	0	0	0	0	0
2017	Written warning	2	0	2	0	1	0
	No. fines	11	0	0	0	0	0
	Value fines	11 248	0	0	0	0	0
	Court cases	0	0	0	0	0	0
2018	Written warning	7	0	0	0	0	0
	No. fines	8	0	0	0	0	0
	Value fines	8 181	0	0	0	0	0
	Court cases	0	0	0	0	0	0
2019	Written warning	0	0	0	0	0	0
	No. fines	0	0	0	0	3	0
	Value fines	0	0	0	0	3 068	0
	Court cases	0	0	0	0	0	0
2020	Written warning	0	0	0	0	3	0
	No. fines	0	0	0	0	6	0
	Value fines	0	0	0	0	6 138	0
	Court cases	0	0	0	0	0	0
As at 31.07.21	Written warning	0	0	0	0	0	0
	No. fines	0	0	0	0	0	0
	Value fines	0	0	0	0	0	0
	Court cases	0	0	0	0	0	0

Bulgarian National Bank

639. For banks, PIs and EMIs, supervisory measures for non-compliance with the legal AML/CFT requirements are imposed with decision of the BNB Governing Council and pecuniary sanctions are imposed with penalty decrees issued by the respective Deputy Governor that is the administrative penalty body. All sanctions are reported to the Governing Council. The BNB has not applied monetary penalties to banks during the review period, nor taken sanctions against persons occupying a senior management role regarding serious and repeated violations. Fines have only been issued for these sectors by the FID-SANS.

640. Except for three fines issued to one EMI in 2021 (total amount of 3 fines is EUR 7669), the sanctions imposed by the BNB were limited to supervisory measures which include: (i) written warnings,; (ii) orders to discontinue and/or rectify breaches within a given time-limit; (iii) order requiring changes in the internal rules and procedures; and (iv) forbidding the conduct of some or all activities until irregularities are resolved under Art. 169(1) of the LPSPS regarding PI/EMIs.

641. Regarding banks, supervisory measures include: (i)written warning; (ii)written orders to cease and eliminate violations; (iii) order requiring changes in the bank's internal rules and procedures or additional requirements for the bank under Art. 103(2), of the LCI.

642. The BNB considers the use of these supervisory measures be an effective method to increase level of compliance as these measures are followed up with action plans and re-inspection to aimed to remedy the identified violations.

Table 6.14. BNB Sanctions - Banks, Payment institutions and E-money institutions

		Inspections (BNB sole)	Inspections (Joint)	Inspections with findings	Number of Orders imposing supervisory measures[88]	Number of fines	Value of fines (in EUR)
2015	Banks	7	3	10	1	0	0
	PIs	0	0	0	0	0	0
	EMIs	0	0	0	0	0	0
2016	Banks	9	2	3	3	0	0
	PIs	0	0	0	0	0	0
	EMIs	0	0	0	0	0	0
2017	Banks	7	0	7	2	0	0
	PIs	0	0	0	0	0	0
	EMIs	0	0	0	0	0	0
2018	Banks	7	0	7	0	0	0
	PIs	3	0	0	0	0	0
	EMIs	1	1	2	13	0	0
2019	Banks	9	1	10	1	0	0
	PIs	0	0	0	0	0	0
	EMIs	1	0	1	4	0	0
2020	Banks	10	8	5	1	0	0
	PIs	0	0	0	0	0	0
	EMIs	0	2	2	0	0	0
31.07.21	Banks	6	1	1	2	0	0
	PIs	0	0	0	0	0	0
	EMIs	1	0	0	0	3	7 669

Financial Supervision Commission

643. A low number of fines have been issued by the FSC and these are not considered to be dissuasive, e.g., maximum amount of fine is EUR 4 500. A large proportion of measures taken by the FSC are recommended actions. Although issuing a recommendation is a positive supervisory action, it is considered neither a remedial action nor a sanction.

Table 6.15. FSC Sanctions

		Inspections (FSC sole)	Inspections (Joint)	Inspections with findings	Supervisory measures issued[89]	Number of issued fines	Value of fines (in EUR)
2015	Securities	2	0	1	3	0	0
	Insurance	3	0	0	0	0	0
	Management companies	1	0	1	9	0	0

[88] Includes written warning, order to discontinue and/or rectify breaches within a given time-limit, require changes in the internal rules and procedures, and forbid conducting of some or all activities until irregularities are resolved.

[89] This is the total number of measures imposed, rather than the number of Orders including measures and also includes written recommendations (i.e., different to the BNB data).

	Pension insurance	8	0	1	6	0	0
2016	Securities	2	0	1	12	0	0
	Insurance	0	0	0	0	0	0
	Management companies	1	0	1	12	0	0
	Pension insurance	10	0	3	0	0	0
2017	Securities	1	0	0	0	0	0
	Insurance	2	0	0	0	0	0
	Management companies	1	0	1	6	0	0
	Pension insurance	1	0	0	0	0	0
2018	Securities	1	0	1	11	1	500
	Insurance	4	0	0	0	0	0
	Management companies	3	0	3	23	0	0
	Pension insurance	0	0	0	0	0	0
2019	Securities	1	0	1	0	0	0
	Insurance	1	0	1	3	0	0
	Management companies	2	0	2	17	2	3 500
	Pension insurance	1	0	0	0	0	0
2020	Securities	4	0	4	32 written recommendations and 1 Coercive Administrative Measure	9	500
	Insurance	-	-	-	-	-	-
	Management companies	2	0	1	9 written recommendations	1	3500
	Pension insurance	1	0	0	0	0	0
2021	Securities	11	2	11	45 written recommendations	41[90]	0
	Insurance	2	0	0	1	0	0
	Management companies	3	2	3	8 written recommendations	2	0
	Pension insurance	2	0	0	4 written recommendations	0	0

National Revenue Agency

[90] Not yet entered into force.

644. The NaRA has powers to issue sanctions to gambling operators only. When breaches are identified, the NaRA may notify the FID-SANS. No statistics have been provided by the NaRA regarding sanctions or other remedial measures taken, notifications made to the FID-SANS or any resulting actions.

Communications Regulation Commission

645. The CRC has no legal powers for sanctioning for the breaches of the AML/CFT legislative requirements. Although the CRC is able to revoke a licence, this can be only done in cases where there is a threat to national security. The CRC is required to report any identified AML/CFT breaches by the PMOs to the FID-SANS. To date, only one case has been referred to the FID-SANS. The CRC reported that it did not have any feedback concerning this referral from the FID-SANS.

6.1.5. Impact of supervisory actions on compliance

646. Impact of supervisory actions on the increased level of compliance by the obliged entities can be demonstrated only to some extent[91].

647. The FID-SANS reported that follow-up inspections demonstrate improvements made by the OEs and generally result in increased reporting of suspicious activity. However, this can be demonstrated only in the case of banks, while other sectors face serious underreporting issues.

648. The BNB focuses its supervisory actions on directing OEs to remediate established violations rather than taking actions to penalise and to deter other OEs. Generally, it considers that this approach yields improvements when entities are re-inspected, however, there have been cases of repeated or similar violations. In such cases either compliance was eventually achieved after significant supervisory effort, or this remains unconfirmed. There does not appear to be consideration given to the root cause of the issue and more severe action taken in cases where failings may be attributed to an inability or unwillingness to comply.

649. The FSC typically identifies only minor violations in its inspections and considers that the level of compliance by its supervised OEs is continually improving. However, in light of the repeated breaches that are commonly found by the FSC, the increasing compliance trends cannot be fully demonstrated across all entities in the supervised sectors.

650. The NaRA is unable to demonstrate the impact of its supervisory actions as no consolidated statistics or case studies are available regarding currency exchange and entities operating in the gambling sector.

651. The impact by the CRC on PMOs level of compliance cannot be proven, reasons being the limited scope of the CRC's supervision (no on-site examinations), general absence of statistics on supervisory actions, AML/CFT breaches identified, and subsequent actions taken, as well as general lack of capacity of the CRC both in terms of resources and expertise on AML/CFT matters.

[91] The assessment of supervisory impact on OEs compliance is largely based on two factors: consolidated statistics on compliance trends (incl. commonly identified breaches and nature thereof) and individual case examples.

6.1.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks

652. There is significant lack of sector specific guidance on implementation of AML/CFT requirements published by the supervisory authorities. Training and outreach activities conducted by the supervisory authorities are not conducted in a systemic manner, are not fully risk based and/ or target the most material sectors. No consolidated supervisory feedback is provided to the OEs on common AML/CFT or TFS breaches.

Training and outreach

653. Throughout the reporting period, the FID-SANS conducted or participated in a number of training events for OEs on AML/CFT. During onsite meetings, OEs were complimentary about the AML/CFT advisory services provided by FID-SANS, i.e., OEs found that FID-SANS were knowledgeable and approachable regarding issues or queries on the practical application of AML/CFT requirements.

654. To date, the FID-SANS trainings appear to have been focused on changes to AML/CFT legislation and preventive measures. Additionally, the FID-SANS provided 12 training sessions regarding the NRA in 2020 (see I.O1). Individual meetings have also been held regarding AML/CFT violations and quality of STRs. However, more targeted outreach on ML/TF typologies and red flags is missing other than the published guidance.

655. Other supervisory authorities' – the BNB and the FSC – outreach activities are mainly based on providing consultations to the supervised population on an ad hoc basis, except the BNB's annual workshops. The FSC increased outreach in 2020 through presentations on CDD, client and transaction monitoring and internal training requirements via its online platform and several thematic training sessions in 2021. No outreach activities have been provided by the CRC and the NaRA. For more information, please see R.34.

General and sector-specific guidance

656. The FID-SANS has published general guidance (applicable to all sectors) on a variety of topics, including the beneficial ownership, PEP-related procedures, compliance control arrangements, new technologies, suspicious transaction reporting and organisation of AML/CFT training for employees.

657. There is currently no additional sector specific guidance issued by the supervisory authorities other than those issued jointly with the FID-SANS and EBA Guidelines published by the BNB and the FSC. Joint FID-SANS and BNB Guidance issued to banks has focussed on red flags regarding TF activities (2016-2017), risk indicators for corruption (incl. PEPs), trade-based money laundering, complex corporate structures and NPOs (in 2021). However, the Joint FID-SANS and BNB Guidance documents are not publicly available; the BNB explains providing guidance directly to credit institutions under its supervision. Thus, there is currently no guidance published by the BNB, the FSC, the NaRA or the CRC other than the provision of links to European guidance on the website of the BNB and the FSC. Some general Guidance was introduced in 2009 and 2012 (relevant until March 2018 when the changes to LMML have been introduced) on STR filing requirements (although this is rather historic and does not address the significant changes introduced by Bulgaria to reflect the new AML regime specified in the LMML).

658. In light of the shortcomings identified under IO4, especially concerning monitoring and assessment of risks, targeted sector specific guidance is a must. The existing guidance for banks also has to be expanded. Please see IO4 and R.34 for more information.

Overall conclusions on IO.3

659. Licencing controls for preventing criminals from entering the market are developed to a good degree for FIs that are supervised by the BNB and the FSC. PMOs, that are weighted most heavily after the banking sector, are subjected to limited market entry requirements. Currency exchange offices, that are weighted third in terms of priority, are not subjected to fit and proper tests regarding shareholders. In the DNFBPs sector, (i) entry controls for shareholders in the gambling sector are applied at a higher threshold than is permitted by the FATF standard and the AT has significant concerns regarding the market entry controls previously conducted by the former gambling regulator which was dissolved following bribery/corruption-related allegations; (ii) heavily weighted sectors, such as the real estate agents, VASPs, trust and company service providers and accountants are not subjected to any fit and proper tests.

660. Risk understanding by the supervisors is varied but generally higher regarding FIs and lower regarding DNFBPs and TF-specific risks. Whilst the AT notes the positive developments by the BNB and the FSC in establishing and enhancing risk-based supervisory models for core financial institutions (amongst which banks are most heavily weighted of all sectors) and payment sector FIs (excluding PMOs), further enhancement is required. Supervision of PMOs, VASPs and currency exchange providers is not risk based and demonstrates very low effectiveness. The supervision most heavily weighted DNFBP sectors (real estate agents, notaries attached to real estate deals, lawyers and accountants that provide company formation and similar services) is not risk-based. Overall, a very low number of inspections of DNFBPs have been carried out during the period under review.

661. The sanctioning regime is complex, and sanctions applied are not proportionate and dissuasive. The supervisors were able to demonstrate that they are making impact on the level of compliance by the OEs to some extent only.

662. A lack of comprehensive and reliable data and statistics required to assess the level of effectiveness with the IO3 has been noted by the AT. This can be partly attributed to a shortage of resources (human, financial, technological) in the authorities which, combined with the duplication of supervision in some cases, prevents supervisors from effectively discharging their duties.

663. Overall, there are major issues regarding market entry controls, risk-based supervision and sanctioning for non-compliance.

664. **Bulgaria is rated as having a moderate level of effectiveness for IO.3.**

7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Actions

Key Findings

a) Bulgarian authorities have a developing level of understanding of the vulnerabilities, and the extent to which certain legal persons created in Bulgaria can be or are being misused for ML/TF. Some legal persons have been identified as being more vulnerable for VAT fraud, TBML (notably in the food or services industry) and ML through construction works. However, this analysis is not comprehensive and does not cover all types of legal persons and legal arrangements and notably does not consider how legal persons are vulnerable to major predicate offences (corruption, OCG activity). The NRA exercise, which covered misuse of some legal persons, was conducted before the introduction of the required beneficial ownership legislation.

b) Bulgaria has fundamental deficiencies in relation to an exercise to convert bearer shares to registered shares with over 40% of entities still to convert shares. Whilst some legislative actions have been taken, the failure to adequately implement this measure is a significant shortcoming.

c) The Bulgarian authorities use several channels to obtain beneficial ownership information on legal persons established under Bulgarian legislation, namely: (i) through information on the registers; (ii) through the obliged entities – mostly banks; (iii) through legal persons on which an obligation is placed to hold BO information. However, all these methods have shortcomings that hinder accessibility and accuracy of BO information.

d) On 31 March 2018, Bulgaria enacted fundamental legal changes implementing a beneficial ownership registration regime of legal persons and arrangements. Under the revised regime, beneficial ownership information is now held alongside basic information (which was previously available) in the publicly available registers and accessible to all competent authorities and obliged entities. However, the Bulgarian authorities were unable to demonstrate that all entities had filed the required information and no processes for BO verification checks were in place. Equally, the very low number of discrepancy reports and the supervisors limited evidence concerning discrepancies between beneficial ownership held by OEs and the information on the register (particularly noting the shortcomings in BO identification – see IO.4) brings into question the effectiveness of this as a mechanism for ensuring information is filed and it is adequate and accurate. This indicates fundamental deficiencies concerning the operation of the new regime.

e) The Registry Agency lacks adequate resources (human, financial, IT) to effectively carry out its functions. The registers rely solely on declarations made in front of a notary by an individual forming a company or amending information to ensure that basic and beneficial ownership information is adequate, accurate and current. The Registry Agency has no legal role in verifying ownership information in the Registry. The Registry Agency do not have legal powers to amend the Register where incorrect information is identified and information is simply sent to the Prosecutors Office (from FID-SANS who received the discrepancy reports). Despite inaccuracies identified, the AT could not confirm whether the Registry has ever been amended.

f) Legal persons established in Bulgaria are not legally required to maintain a business relationship with a Bulgarian OE. It is therefore not possible to rely upon OE's to provide basic and BO information in all circumstances. Even in cases where beneficial ownership information is available from the OEs, it is considered that BO data held by OEs might not always be reliable (see IO.3/4). Moreover, the supervisory regime is not fully effective which further hampers accuracy of BO information held by the OEs. Linked to this, a regulatory regime for TCSPs is not established in Bulgaria and the population of lawyers and accountants conducting TCSP activities as covered by the FATF standard is not known.

g) The use of straw men is a significant risk to Bulgaria; however, the authorities have not taken sufficient action to prevent against the use of informal nominee relationships as straw men. Whilst Bulgaria does not provide for the existence of formal nominees in legislation, there are no verification mechanisms to check for nominee arrangements. However, even in a situation where nominee arrangements were found, there is no legal prohibition for their existence and thus no legal grounds to initiate proceedings.

h) The Bulgarian authorities were unable to demonstrate that effective, proportionate and dissuasive sanctions had been applied against persons not complying with the requirements relating to basic and beneficial ownership information. Aggregated statistics provided indicate a low total level of fines.

Recommended Actions

a) The authorities should conduct a more detailed analysis of ML/TF risks associated with all types of legal entities. This should particularly focus on the use of "straw men" in Bulgaria and build upon the analysis in the NRA which indicates where legal persons may be vulnerable to ML/TF. In addition, analysis should extend to the cross-border ML/TF threats, including the underlying predicate offenses with a particular focus on high-risk predicates, most notably corruption. The Registry Agency should be a key part of that assessment.

b) Bulgaria should urgently review the process in place to ensure the transition of bearer shares to registered shares. Bulgaria should put in place a process to complete this transition quickly with a verification exercise for persons that have not complied with the bearer shares registration requirements. Proportionate and dissuasive sanctions should be applied for failure to register shares.

c) An urgent review should occur to address fundamental deficiencies in the operation of the registers ability to hold accurate and current beneficial ownership information. The review should look to focus on an effective mechanism for ensuring accuracy of information on the Registers and adequate monitoring and enforcement procedures for failure to update the registers. The review should deliver a mechanism to ensure all legal persons and arrangements obliged to file information under the LMML have filed such information. The Review should also deliver an effective mechanism to correct incorrect information on the Register in a timely manner – considering the reporting mechanism for discrepancies and whether the Registry agency have adequate powers to amend the Register.

d) The role, structure and human resources of the Registry Agency should be reviewed to ensure it has the ability to implement verification measures to ensure that beneficial ownership is accurate and up to date; the Registry agency should be granted necessary resources (human, financial, IT) to achieve these goals.

e) Bulgaria should either explicitly prohibit nominee arrangements and establish verification mechanisms to check for nominee arrangements or introduce an appropriate registration regime to record nominee arrangements. Proportionate and dissuasive sanctions should be in place to enforce these provisions.

f) Bulgaria should look to strengthen enforcement measures concerning beneficial ownership information, particularly to ensure information filed in the Registers is checked and found to be accurate and up to date (including being updated upon change). Proportionate and dissuasive sanctions should be applied for: (i) failure to provide accurate basic or beneficial ownership information; (ii) providing false information to the Registry. Consideration should be given to a requirement to enhance discrepancy reporting and to regularly confirm that no changes in beneficial ownership information have occurred.

g) Bulgaria should review the range of sanctions available for failing to comply with information requirements to ensure they are effective, proportionate and dissuasive in all circumstances. There should be a general review of the ability of the system in Bulgaria to effectively implement sanctions for failing to comply with information requirements given the current very low numbers, value and low percentage of fines settled. Supervisory authorities should also ensure they take proportionate and dissuasive action against obliged entities that fail to maintain adequate, accurate and up to date information.

h) Bulgaria should establish registration regime for the TCSPs and enhance monitoring of the TCSPs with the AML/CFT requirements, especially concerning beneficial ownership.

i) Bulgaria should take actions to address technical deficiencies relating to transparency of legal persons and arrangements (R.24-25) which inhibits the effectiveness of the overall regime.

665. 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 RR.24-25, and elements of R.1, 10, 37 and 40.[92]

7.2. Immediate Outcome 5 (Legal Persons and arrangements)

Contextual Information

666. The Bulgarian legal framework provides for the establishment of the following types of legal persons: General partnership; Limited partnership; Limited liability company; Sole-owned limited liability; company; Joint stock company; Sole-owned joint stock company; Special investment purpose companies; Limited stock partnership; Cooperatives; State Undertakings; Public Undertaking Merchant; European economic interest grouping (EEIG); European Cooperative Society; European Company (Societas Europaea); Companies registered in preferential tax regime jurisdictions; Branch of a foreign legal entity; Association; Foundation; Branch of foreign NPO; Community Culture Center. The legal framework does not provide for the establishment of trusts or other forms of legal arrangements in Bulgaria; however, foreign legal

[92]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.

arrangements can be administered in Bulgaria. The Table 7.1 below provides the number of legal persons broken down by type as of July 2021.

Table 7.1. Legal persons at the Commercial Register[93]

Type of Legal Persons / Arrangements	Number
General partnership	6171
Limited partnership	101
Limited liability company	186842
Sole-owned limited liability company	578767
Joint stock company	9431
Sole-owned joint stock company	3369
Special investment purpose companies	67
Limited stock partnership	27
Cooperative	3517
State Undertakings	18
Public Undertaking Merchant	3
European economic interest grouping (EEIG)	18
European Cooperative Society	1
European Company (Societas Europaea)	3
Companies registered in preferential tax regime jurisdictions	40
Branch of a foreign legal entity	604
Association	15378
Foundation	2917
Branch of foreign NPO	110
Community Culture Center	2642

7.2.1. Public availability of information on the creation and types of legal persons and arrangements

667. Information on the creation and types of legal persons and legal arrangements that may be established under Bulgarian legislation is publicly available. The relevant legislation provides information on the types and features of the legal persons and arrangements and is publicly available.

668. Information on the processes for the creation of legal persons can also be found online on the website of the Commercial Register and register of non-profit legal entities. The Registry Agency operate a United portal for request for electronic administrative services (https://portal.registryagency.bg/CR/en/services). This contains information on the type and form of the submitted documents required by the Registry Agency to create legal persons in Bulgaria.

7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

669. Bulgaria has conducted a significant NRA exercise publishing a NRA report in 2020. Bulgaria has a developing level of understanding of the vulnerabilities, and the extent to which

[93] Bulgarian authorities suggest that relatively large number of LLCs (incl. sole-owned) compared to the population can be explained by the fact that some persons potentially own multiple companies. No additional information, e.g., rationale / purpose, business activities was made available to the AT.

certain legal persons created in Bulgaria can be or are being misused for ML/TF. The NRA generally recognises that legal persons established in Bulgaria represent the second highest number of subjects involved in potential ML activity, with the average volume of cases significantly higher than for natural persons. Some legal persons have been identified as being more vulnerable for VAT fraud, TBML (notably in the food or services industry) and ML through construction works. The risk assessment also acknowledges that the LLC structure is particularly vulnerable to abuse, including the sole owner LLC which is the simplest formula to be used with a single "straw-man" as its owner. It equally acknowledges vulnerabilities to PEPs and PEP related criminal groups for complex money laundering schemes involving foreign legal persons and finally notes these can be used as "shelf" or "shell" companies for tax evasion/tax fraud or related ML purposes. The NRA does note how the banking sector may be misused by Bulgarian legal persons to facilitate ML generated from tax offences (including VAT related crimes) and fraud; that the real estate sector may also be misused by legal entities; and finally, that lawyers, notaries and accountants may be involved in professionally enabling ML by setting up legal persons in Bulgaria.

670. However, the NRA process does not represent a comprehensive and systematic analysis of ML/TF risks associated with all types of legal persons in Bulgaria. The current analysis of the inherent vulnerabilities of each relevant type of legal entity is currently not complete, is very much driven by recent operational activity by the authorities is relatively limited in covering the exposure of all entities to risk. The analysis focusses around the structure, type of entity and its owners with some consideration of activity of the entity. However, it is more limited on considering how different sectors of the financial and non-financial sector may be exposed to ML/TF risks through the misuse of legal entities. Whilst some legal persons are noted as being vulnerable to certain types of major predicate offences, the NRA does not consider in detail how legal persons may be vulnerable to ML from corruption or OCG activity which are major areas of risk for Bulgaria.

671. A further significant shortcoming in the current understanding of legal persons vulnerabilities in Bulgaria is the fact that the data for the NRA exercise (and a large proportion of the analysis) was taken from before the changes to the LMML were introduced in 2018 creating the new beneficial ownership information regime.

672. The level of understanding did vary across the authorities. Some authorities, particularly sector supervisors such as the BNB demonstrated a more developed knowledge of the vulnerabilities of legal persons and arrangements that the banking sector is exposed to which went beyond the NRA. Other authorities demonstrated a more general understanding that did not extend beyond the NRA. Banks met onsite confirmed that Bulgarian registered companies with foreign UBOs was the most prevalent typology featuring in their STRs. However, information on number of companies with foreign UBOs is not available in the country.

673. The Registry Agency is not represented in the NRA WG and had very limited role in the risk assessment process so far in Bulgaria. The Registry Agency now act as the key gateway for registration of legal persons and arrangements and filing of BO information. However, the functions of the Registry Agency do not extend to considering risk that legal persons and arrangements present in Bulgaria. Therefore, the Registry Agency has no formal role in understanding ML vulnerabilities, and the extent to which legal persons created in Bulgaria can be or are being misused for ML/TF exists. Whilst the Registry Agency presented a compelling position that they fulfilled all of their designated functions, they clearly outlined they were not empowered to consider risk factors in the refusal of BO registration. The AT consider this to be a

fundamental deficiency in the Bulgarian regime. The Registry Authority was also unable to produce specific data (on many occasions due to inadequacy of IT systems and/or due to the fact that some statistics is not being collected) which would assist in understanding ML/TF vulnerabilities in Bulgaria of legal persons/arrangements.

674. The AT therefore considers that the authorities have a developing understanding of the vulnerabilities of the current regime in place and the extent to which legal persons created in Bulgaria can be or are being misused for ML/TF. The Bulgarian authorities should urgently consider the ML and TF threats and vulnerabilities associated with all types of legal persons and legal arrangements in Bulgaria in a systematic manner and particularly focus on those major predicate offences (corruption/OCG) where legal persons may be used but have not yet been examined for vulnerabilities.

7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements

675. Bulgaria has several measures by which it has sought to prevent the misuse of legal persons and arrangements.

Sources of BO information

676. The Bulgarian authorities use several channels to obtain beneficial ownership information on legal persons established under Bulgarian legislation, namely: (1) through information on the various registries which hold beneficial ownership information; (2) through the obliged entities – mostly banks; (3) through the legal entity itself and/or the natural person contact point. However, all of these methods have shortcomings that hinder reliability and accuracy of BO information, as discussed below.

Registry

677. In order to enhance the transparency of legal persons and arrangements and further to the requirements to implement relevant EU Directives, on 31 March 2018, the amendments of the LMML came into force introducing the requirement for a register of beneficial ownership of legal persons and arrangements. In 2019, a beneficial ownership register was established and brought into force (achieved through the addition of a separate section to the Registers concerning beneficial ownership). Currently there are 3 registers that contain basic and beneficial ownership information on the legal persons or trustees of a foreign law trust, namely, Commercial Register, the Register of Non-Profit Legal Persons Act and the BULSTAT Register.

678. The AT commend the Bulgarian authorities for this significant action which has enhanced the beneficial ownership transparency regime in Bulgaria. However, the AT is concerned that the process for the changes to the regime has not been comprehensively implemented in order to ensure that all legal persons and arrangements have filed basic and beneficial ownership information to the Registry. There has generally been no process to check that filing has been completed in line with the legislative provisions. There are no statistics available on how many BO filings have been received; no verification checks on the beneficial owner submitted by the legal persons are carried out by the Registry Agency.

679. Equally, the AT have fundamental concerns that the role of the Registry Agency, who administer the relevant registers, is not yet adequately defined, structured, and sufficiently resourced. The Registry Agency currently have very little engagement with national AML/CFT policies, co-ordination and risk assessment and this exacerbates a vulnerability in the Bulgarian regime.

680. Moreover, the AT are of the opinion that significant lack of resources hampers the effectiveness of Registry Agency's work in ensuring availability of accurate and current BO information. It was confirmed that there are 119 Registry Agency staff dedicated the work of registering legal entities and arrangements. Their role is to check that information complies with the legal requirements for submission and checks are made against documents filed in the Notary system to ensure authenticity of documents. Their work does not involve any role in verification of the accuracy of documents. In addition, it is of note that: (a) no additional human resources have been granted to the Registry to carry out BO registration exercise; this is crucial given large number of entities operating in Bulgaria (see Table 7.1); (b) no additional technical resources have been considered (e.g., although legal persons are legally required to provide information to the Registry on citizenship of the BOs, no related statistics could be made available to the AT the reason being that the citizenship/residency information cannot be retrieved from the IT systems currently used by the Registry); (c) no additional financial resources were granted to increase expertise of the Registry officers who are tasked with entering of BO data into the systems, i.e., no trainings, instructions on verification checks, etc. provided; and no mechanisms established by the country to conduct verification checks of the BO data received. This is of a particular concern to the AT given the complexity of the BO definition and related beneficial ownership identification issues that would require expertise of the Registry officer who enters the BO data into the system so to enable him/her to critically assess whether the information submitted is adequate (especially in relation to persons that do not meet beneficial ownership threshold and/or are controlling senior manager officials in the absence of a natural person who holds 25 % and more of the shares, etc.).

681. The above-mentioned points (a-c) were fundamental to ensure the quality of BO information held on the Registries in Bulgaria. These deficiencies are particularly concerning to the AT, who consider that this area should be of the highest priority given the context of Bulgaria, where the use of legal persons, including the use of "straw men" through legal entities, is one of the most prevalent ML typologies.

682. Another fundamental deficiency of the BO transparency regime is the absence of the explicit legal requirements to declare all legal owners, i.e., legal persons (other than ultimate beneficial owners who are natural persons) that own the entity by holding certain percentages of shares. The minimum information accessible at the Registry is (1) the first layer of owners (be it ultimate beneficial owners or legal owners) and (2) the ultimate beneficial owners natural persons (be it in the second, third or any other ownership layer). This therefore means that the Bulgarian system focusses predominantly on direct ownership with deficiencies in registration of indirect ownership. Indirect ownership though can always be captured where legal owners are Bulgarian entities the reason being that all legal persons established in Bulgaria have to report their beneficial owners. Although Annex to RILMML provides for a template for BO reporting, including BO structure, it is not clear whether this can be enforced. Direct examples were given on-site particularly by lawyers/accountants concerning the lack of need to register indirect layer of ownership. For more information, please see section 7.2.4., particularly concerning a role of notaries.

683. Whilst the introduction of registers is a positive step forward, fundamental deficiencies in their implementation prevent them being particularly effective at the current time in preventing the misuse of legal persons and arrangements in Bulgaria.

Role of the FIs/DNFBPs

684. To some extent, the FIs/DNFBPs and the supervisory regime may prevent against the misuse of legal persons and arrangements for ML/TF. The most relevant sectors in this respect is banking sector end entities (lawyers and accountants) that provide trust and company formation services.

685. For mitigation purposes, the OEs acting as a gatekeeper is looked at from two different angles: (1) OEs role in identifying beneficial owners and keeping information up to date (consequently making this information available to the competent authorities upon request); (2) OEs role in identifying suspicious patterns of activities and transactions involving legal persons and notifying the FID-SANS by way of an STR. However, both of these roles by the private sector appear to have deficiencies.

686. First, it is not possible to confirm that beneficial ownership data of the Bulgarian legal persons are always held by the OEs due to the following factors: (a) although the legal persons are legally required to deposit share capital before registering legal person into the Bulgarian bank by opening an account, this requirement does not extend throughout the lifetime of the legal persons (i.e., bank account can be closed upon registration); (b) legal persons are not legally required to engage a CSP (lawyer and/or accountant) to register a company; moreover, the statistics on how many Bulgarian registered legal persons have sought services of the CSPs in Bulgaria are not available. Due to the above reasons, it is not possible to confirm that information on BOs can be obtained from the OEs in all cases. Also see IO4.

687. Second, even in cases where beneficial ownership information is available from the OEs, the evidence (based on the shortcomings that relate to the implementation of the BO legal requirements by the OEs) suggests that BO data held by OEs might not be always reliable. There is a good understanding by banks and other OEs of beneficial ownership requirements; however, much of the verification process reverts to beneficial ownership information held on the registries which in the view of the AT has fundamental issues with accuracy of information. Some OEs had identified discrepancies with data in the public register and some noted difficulties in establishing the ultimate beneficial owner in cases where structures are complex.

688. Third, risk understanding significantly varies sector by sector. The BNB and banks in Bulgaria have a reasonable understanding how they can be misused for ML/TF by legal persons and arrangements. Banks commonly report Bulgarian established legal persons featuring in ML schemes which is the most prevalent typology featuring in the STRs filed by banks. Other FIs and the FSC have a basic understanding how they can be misused for ML/TF by legal persons and arrangements, however, this understanding needs to be further developed. The knowledge of the FID-SANS about how the DNFBP population they supervise may be misused by legal persons/arrangements is limited and the knowledge of the legal and accountancy sector is also not developed.

Role of the Supervisors

689. The FID-SANS for DNFBPs and the BNB for banks provides a level of prevention against misuse, although this is very basic in nature and varies significantly across sectors. The 2020 NRA report noted the particular risk to the legal sector, since lawyers and accountants are often engaged in the setting up of companies and provide other company services. It also noted the potential for both lawyers and accountants to be involved in complex ML schemes due to their involvement in planning and execution of such schemes. Bulgaria notes that some actions to address these issues with the Supreme Bar Council and the Institute of Certified Expert-Accountants have been undertaken.

690. However, as noted under IO3, supervision of lawyers, accountants and TCSPs is generally weak. This is partly attributed to the fact that no consolidated data is available on how many lawyers and accountants conduct FATF covered activities, incl. trust and company services; and significant shortcomings exist in the licensing regime of the aforementioned professions; this, combined with the limited risk understanding in these sectors, does not allow for allocation of the supervisory measures which are targeted and sufficient, both in terms of scope and frequency. See IO3 for more information.

691. A total of 32 BO information related infringements by the OEs[94] have been established by the FID-SANs in 2015-2020 with some minor sanctions established (please see section 7.2.6 for more information). In addition, 11 on-site examinations carried out by the BNB found violations relating to breaches of identification and verification requirements of the beneficial ownership by the OEs in the period 2015-2018 (no infringements identified in 2019-mid-2021); it is not possible, however, to accurately confirm the types or severity of these breaches on the available data.

692. In general, as noted under IO3, sanctions applied by the supervisory authorities for AML/CFT breaches by the obliged entities are not considered to be dissuasive and proportionate. It is particularly of note that for a matter to be a repeated breach (in which cases more dissuasive sanctions should be applied), it had to be identified more than once in a single year (as per legislative requirements), meaning this is very unlikely to be discovered.

693. Given the limited effectiveness of the supervision by the FID-SANS over DNFBPs, low number of inspections and infringements identified in this area by all supervisors, it can't be considered that the supervisory regime is an effective mechanism on protecting against misuse of legal persons and arrangements in Bulgaria. Whilst supervision provides a level of prevention against misuse, in light of the risk context in Bulgaria, this is not considered sufficient.

Conversion of bearer shares

694. Whilst legislative amendments have been made concerning Bearer Shares in Bulgaria, in practice fundamental deficiencies exist in relation to an exercise to convert bearer shares to registered shares with over 40% of entities still to convert shares. Whilst some legislative actions have been taken, the failure to adequality implement this measure is a significant shortcoming.

695. Through an amendment of the Commercial Law (SG № 88 from 2018, effective from 23.10.2018) the possibility for the joint stock companies and for partnerships limited by shares to continue to issue bearer shares has been revoked. The provisions also stipulated that bearer shares issued prior to the entry into force of the law shall be replaced by registered shares and that within nine months of the entry into force of the law, companies that issued bearer shares or substitute interim certificates shall amend their Articles of Association, replacing the bearer shares or substitute interim certificates with registered shares. There was also the requirement for those entities to commence keeping shareholders registers, declare the changes and submit the amended Articles of Association to the Commercial Register. The legislation required a shareholder to submit the bearer shares owned for replacement or the company is required to invalidate the shares. Companies that failed to comply with this obligation can be terminated pursuant to Art. 252, paragraph 1, item 4 of the Commercial Law with decision by the Court upon

[94] Only OEs covered by the FATF standard are included here, thus excluding other OEs under the Bulgarian AML/CFT laws.

a request filed by the prosecutor. All companies were required to change bearer shares with registered by 23rd July 2019.

696. Although the data confirming the completion of this exercise was not available during the onsite visit[95], the authorities further confirmed that 921 of the JSCs with bearer shares have converted their shares to registered ones. However, the remaining 638 of the JSCs still have not converted their shares to bearer shares.

697. The Prosecutor's Office noted that a file was opened in the Supreme Prosecutor's Office of Cassation. As the list of companies included those based in the whole country, they were divided into district cities in the Republic of Bulgaria and sent to 26 district prosecutor's offices with instructions to take action. The authorities informed the AT that all companies were inspected, and different decisions followed, however, it was not demonstrated to the AT that these actions have resulted in concrete actions to bring the status of the JSCs in line with the law or strike off the entities. The AT considers that this is particularly concerning given the deadline had elapsed by over 2 years and this exercise along with the role of the various agencies in completing it should be urgently reviewed.

Requirements on nominee shareholders/directors

698. Whilst Bulgaria does not provide for the existence of formal nominees in legislation (see also c.24.12), the NRA report outlined as one of the high-risk ML events that the laundering of illicit funds using shell companies and informal nominees (straw men) particularly for tax evasion and VAT fraud, and equally in the food and oil trade market (particularly relying on a corrupt environment and informal economy) was a significant risk to Bulgaria. The Registry agency does not have verification mechanisms to check for nominee arrangements. However, even in a situation where nominee arrangements were found, there is no legal prohibition for their existence and thus no legal grounds to initiate proceedings.

Outreach measures to enhance accuracy of BO information

699. The Bulgarian authorities reported that they have taken a number of outreach measures to ensure adequate, accurate and current basic and beneficial ownership information on legal persons and arrangements is available in the country. The authorities (FID-SANS, FSC, BNB) noted that they have conducted sessions on the topic of the definition of a beneficial owner, the different scenarios for beneficial ownership, as well as the technical arrangement regarding the filling in of the declaration for beneficial owner, the registers which can and shall be consulted, the types of documents which might assist the obliged entities in identifying the beneficial owners. For example, under the review period, the FID-SANS has trained banks on this topic in 2016 and 2018 (5 seminars delivered, 125 persons from the banking sector trained), 1 training organised for other FIs in 2016 (20 persons trained), 1 training for investment sector in 2018 (35 persons trained); trainings are also provided to some of the competent authorities, such as Customs Agency, FSC, Privatisation Agency, Persons who organise procurement orders, etc. The FSC conduced intense outreach in 2021 on ML/TF topic also covering BO information as part of a general ML/TF training. However, the vast majority of the sectors, especially the most heavily weighted ones (such as money value transfer businesses, virtual asset service providers, currency

[95] After the expiry of the relevant deadline in the Commercial Act (23rd July 2019), the Registry Agency sent to the Prosecutor General of the Republic of Bulgaria a list of the JSCs that have not fulfilled their obligations to replace bearer shares with registered ones. These actions have commenced after the on-site, October 2021.

exchangers, real estate sector, TCSPs, etc.) have not been covered. In addition, there is not enough evidence that the outreach was specifically designed to cover BO topic extensively and has taken into account the contextual factors of Bulgaria, including those related to complexity of legal and beneficial ownership structures, etc.; also, there is no evidence that the outreach was intensified following the regulatory amendments relating to the legal and beneficial ownership regime (including abolishment of bearer shares, introduction of BO register, requirements on discrepancy reporting, etc.).

700. Bulgaria has therefore made some efforts to indicate to industry the main changes made by the LMML and RIMML but it is unclear the extent to which these have filtered through into the beneficial ownership regime in the country.

701. In respect of NPOs, specific guidelines were developed for the NPOs, which are aimed to adapt the legal requirements to the nature and type of their activities and to reduce any unnecessary administrative burden on these organizations. Specific outreach has occurred with the Bulgarian Center for Non-Profit Law to guide the NPO sector on these issues and assist them in fulfilling their obligations.

7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

702. Competent authorities can obtain access to basic and beneficial ownership information through one of the three methods: (1) checks in the respective publicly accessible registers; (2) through a request to the obliged entity about the respective legal person or entity it has a business relationship therewith; (3) through a request to the respective legal person or a contact point natural person.

703. Basic and beneficial ownership information on legal persons is available to all competent authorities through a direct online access to Commercial Register and Register of the Non-Profit Legal Entities or the BULSTAT Register, depending on the type of legal person; and is easily accessible through the Registry Portal (https://portal.registryagency.bg/CR/en/services). The Registry portal allows for information to be found on company identification number, name, legal form, registered office, scope of business activity, directors, and ownership capital. Access to the information in the registers is public[96], thus also accessible to all OEs. As far as the registers are electronic, the available information is adequate and current up to the time of the check made.

704. Although no consolidated statistics is available on how frequently each of the three channels are used to obtain basic and beneficial information by the competent authorities (supervisors, the FID-SANS and LEAs), authorities report that the first two sources are used most frequently, i.e., through OEs and Registry. Although the LEAs tend to rely on data held at the registers[97], the FID-SANS confirmed is also seeking information from the OEs, mainly banks.

[96] Authorities have informed that only personal data is not accessible due to the data protection requirements. However, no information was provided on data set that is not accessible.

[97] Including BULSTAT and CRRNPLP register – for the access to all documents uploaded on the files of each legal person and other legal entity, incl. financial statements; APIS Register information – third-party held register with information
for establishing commercial links between natural and legal persons, financial analysis function.

There were cases of discrepancies identified between BO data held by the Registry and BO data held by OEs.

705. No consolidated data and statistics provided by the authorities on: (1) the use of the third method; (2) requests to the OEs and number of checks in the Registry; (3) as well as no statistics or consolidated observations on the timeliness of the feedback from the OEs or the legal entity itself.

Accuracy of information held in the Registry

706. On 31 March 2018, the LMML extended the requirements to cover beneficial ownership information on legal persons and arrangements which is also held on the Commercial Register and Register of the Non-Profit Legal Entities or the BULSTAT Register, depending on the type of legal person. Legal persons, as well as the natural contact persons (where applicable) were required to submit information on their beneficial owners by the 1st February 2019 to the relevant Register.

707. The following beneficial ownership information is legally required to be entered into the register concerning identification of the beneficial owner: name; citizenship; unified civil number for the persons under Art. 3(2) of the Civil Registration Act; date of birth for the persons, other names; state of residence, if different form the Republic of Bulgaria or from address. In addition, information about the legal entities chain of ownership, including any individual exercising direct or indirect control over the respective legal person should be filed. However, information publicly displayed on the register is simply the name of the beneficial owner, which does give the AT cause for concern regarding the factors that can be used to verify ownership that are publicly available.

708. A critical factor in the legal persons transparency regime in Bulgaria is the verification of the BO data entered into the Registry. Authorities reported that involvement of a notary should be considered a verification measure, however, it was ascertained by the AT that the role of a notary is limited to certifying the identify and the signature of the representative of the legal person who is filing documentation to the Registry; thus, notaries provide no independent role in verifying the overall beneficial owners of the legal persons. Equally, there was not a process in place at the Registry Agency to systematically ensure that all legal persons had filed beneficial ownership information, nor verification of such information.

709. According to the legal requirements, the information on beneficial ownership will only be entered onto the Registers upon a notarized declaration signed by the legal representative of the legal person. The template of the declaration is provided in Appendix 3 of the RILMML. The declaration must involve description of the beneficial ownership but there are no provisions on the exact description details. The Bulgarian authorities note that the declaring legal representative is responsible for describing the beneficial interest accurately and clearly. There are equally requirements under the LMML that information on beneficial ownership must only be entered onto the Registers with consent of the individuals. It is therefore questionable what happens in terms of either refusal of the consent of the individual or process to confirm that the individual has actually consented. The AT were not presented with any examples of these situations.

710. The AT met with the Registry Agency and a variety of Notaries to analyse the process for notarising the beneficial ownership declaration. The Notaries work relates to a declaration under Art. 38 of the RILMML and the consent of the natural contact person under Art. 63(4)(3) of the LMML. Whilst the notaries may check documents concerning the basic ownership information,

there is no checking of reliable, independent source documents, data or information when notarising the beneficial ownership information. The work of the notary will simply involve verification that the legal representative of the legal person is properly identified, which often occurs using the notary passport verification system and a confirmation of the content of the declaration that the legal representative is making. The Notaries operate under the Notaries and Notarial Practice Act and a set of Uniform Internal Rules for the control and prevention of money laundering and terrorist financing. The AT examined the provisions of legislation and the internal rules and it is clear that the role of the notary is to solely certify the identify and the signature of the representative of the legal person who was filing documentation. On occasion that would be the managing director/legal representative, but this would not include separate identification of the beneficial owners of the legal person. Whilst on occasion, the notary may see documents relating to the overall ownership structure of the legal person, they are not obliged to check the beneficial ownership or confirm the structure. The AT consider it clear from on-site interviews that the notaries do not consider their role and obligations to extend beyond verifying the identity of the managing director/legal representative of the legal person and explaining the content of the declarations.

711. There was not a process in place at the Registry Agency to systematically ensure that all legal persons had filed beneficial ownership information. The Registry Agency also conduct no independent verification process on the accuracy of the information submitted on beneficial ownership. The Registry Agency officials confirmed this was not part of their current mandate, where the only requirement involved a cross-check under Art. 21(8) of the ACRRNPLER. Consequently, there are no statistics available concerning the completeness of filing of BO information. Therefore, Bulgaria is unable to confirm that all entities have filed beneficial ownership information and appear to rely upon future discrepancy reporting to identify issues with the adequacy of registration. The AT consider this to be a major deficiency in the implementation of the beneficial ownership regime in Bulgaria.

712. The AT therefore consider that Bulgaria has put in place no effective mechanism to ensure that beneficial ownership information held on the Commercial Register is accurate as there is no process where it can be verified against reliable, independent source documents, data or information. This fundamental deficiency is exacerbated when considering that the main private sector source of verification of beneficial ownership of legal persons in Bulgaria is reference back to the Commercial Register and Register of the Non-Profit Legal Entities or the BULSTAT Register.

Accuracy of information held by the OEs

713. Whilst the Bulgarian authorities note that the identification process is complete only when the obliged entity is satisfied that there is no doubt in the identification of the beneficial ownership, some practical concerns remain. As noted under IO4, all OEs met onsite were familiar with legal requirements regarding beneficial ownership and control taking the practical steps to establish and verify ownership included by a combination of means consisting of obtaining self-declarations from the client, certified copies, legal documents including articles of associations and checking against the Commercial Register. However, some entities had identified discrepancies with data in the public register and some noted difficulties in establishing the ultimate beneficial owner in cases where structures are complex. For example, lawyers met onsite stated often finding errors in the Registry, information on all legal owners might not be accessible (specifically mentioning the example of the JSC the shareholders of which are legal persons). Auditors echoed concerns expressed by the lawyers by stating that the BO registry is not fully complete, especially concerning information on large international groups.

714. The Bulgarian authorities also note that when discrepancies occur, banks, payment institutions and e-money institutions request additional information/correction of the filed documents within the CDD procedure and take appropriate measures. The AT found that occasionally discrepancy reports were filed with the Commercial Register – although only FID-SANS had the ability to take action related to those discrepancy reports. Upon identification of discrepancies between CDD data on beneficial owner submitted by the clients and information on beneficial owners contained in the registers, OEs are legally required to notify the FID-SANS. Under the review period, the FID-SANS has received 4 discrepancy reports from the OEs. The authorities stated that most discrepancies were due to technical mistakes made when the legal persons submitted the relevant information to the register. This raises concerns about the accuracy of the data entry on the Registers. Consequently, this might negatively affect OEs' ability to verify the beneficial ownership information, as the majority of the OEs use the various registers as their main source for confirming (verifying) basic and beneficial ownership information on legal persons in Bulgaria. Equally, the AT were concerned by the very number of discrepancy reports and the supervisors limited evidence concerning discrepancies between beneficial ownership held by OEs and the information on the register (particularly noting the shortcomings in BO identification – see IO.4)

715. Finally, it was established that the Registry Agency do not have legal powers to amend the Register where incorrect information is identified (unless there is a court order or a new application by the legal entities) and information is simply sent to the Prosecutors Office (from FID-SANS who received the discrepancy reports). Despite inaccuracies identified, the AT could not confirm whether the Registry has ever been amended and which competent authorities are authorised to introduce changes to the Registry. This raises fundamental questions as to the accuracy of the Register and how it can reasonably be used to verify beneficial ownership information by OEs.

Current Information

716. Art. 61(1) of the LMML requires all legal persons and natural contact persons to obtain, hold and provide adequate, accurate and current information on their beneficial owners. Updating the Registers is also covered by Art. 63(4), item 4 of the LMML requiring any changes in the data and information about the beneficial ownership to be provided. Pursuant to Art. 6(2) of the ACRNPLER and Art. 12(4) of the BRA, the deadline for submission of application for entering any changes in these register (which includes cases referred to Art. 63(4)4 of the LMML) is 7 days after the change. However, as noted above, the Registry Agency has no process in place to verify whether information on BO changes is submitted.

717. Whilst the 7 days deadline is short, the private sector appears to have limited knowledge of the obligation to file changes in beneficial ownership information in the given timeframe and the Registry Agency have no enforcement function to check that filings are made when information changes. The Registry Agency appear to rely upon discrepancy reporting as the only method in which to become aware of information that is not accurate on the Register due to change. The AT therefore consider this represents a major deficiency in Bulgaria as to the ability to gain timely access to a current beneficial ownership information.

7.2.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

718. Generally, the same provisions as outlined in the section 7.2.4 apply to legal arrangements in Bulgaria, i.e., the same fundamental deficiencies exist as for legal persons, particularly

concerning the Registers, however, the situation is significantly less material for the country in respect of legal arrangements when compared to legal persons.

719. Bulgarian legislation does not explicitly provide for the existence of trusts, however, the authorities acknowledge that foreign trusts and other similar foreign legal arrangements, established and existing under the law of the foreign jurisdictions, which permit such forms of trust ownership, may operate within the territory of the Republic of Bulgaria. The basic and beneficial information on the legal arrangements can be accessed through two channels: Register and the OEs, including trustees.

720. First, trustees are legally required to hold accurate and current BO information which is entered to the BULSTAT Register. However, as at the time of the on-site visit, the AT was informed that no registration of this kind existed in the BULSTAT Register.

721. Second, although trustees of a foreign law trust in Bulgaria are OEs and are required to comply with the CDD and record keeping obligations, the following circumstances might hinder the access to basic and beneficial information on legal arrangements: (1) trustees are not explicitly required to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors and managers, accountants and tax advisors; (2) there is currently no legal mechanism in place to identify those who are conducting trustee services and therefore the population of trustees is unknown. For this reason, the authorities are unable to identify trustees and thereby obtain timely access to information from trustees.; (3) trustees are not required to disclose their status to FIs/DNFBPs when forming the business relationship.

7.2.6. Effectiveness, proportionality and dissuasiveness of sanctions

722. The Bulgarian authorities were unable to demonstrate that effective proportionate and dissuasive sanctions were applied against persons who do not comply with information requirements.

723. Some actions have been taken in relation to cases of: (1) BO inaccuracy identified through discrepancy reporting; (2) BO infringements by the OEs and subsequent sanctions applied by the FID-SANs; (3) failures to submit basic information and BO information for newly formed companies.

724. In 2019-2020 the FID-SANS was informed 4 times on discrepancy between the natural person listed in the Commercial register as beneficial owner and the one identified when conducting CDD by the OEs. Information on three of these cases was disseminated by competence to the Bulgarian Prosecution. Data on the fourth case was disseminated to the Registry Agency for administrative-penal measures.

725. A total of 32 BO information related infringements by the OEs[98] have been established by the FID-SANs in 2015-2020. Although FID-SANS report that in 2014 – 2020 a total amount of fines imposed reached € 57 009 and 2 warnings were issued, these sanctions were in combination for other AML/CFT related breaches and thus does not solely refer to establishing the identity of the client legal person and its beneficial owner(s). It could be only ascertained that 2 accountants have been fined for breaches of BO related requirements (fines amount to € 3 068 and € 6 136 respectively).

[98] Only OEs covered by the FATF standard are included into statistics.

726. However, the total number of infringements appears very low, which, combined with the extremely low number of cases of discrepancy reporting (as discussed above), does not seem reasonable in light of the context of Bulgaria.

727. In general, very low number of cases relating to failures to submit basic and beneficial ownership information to the Registry have been identified. Fines settled for these infringements are not dissuasive. Apart from administrative penalties and 4 cases of strike off of the companies, no other sanctions have been imposed. Authorities reported that in the period of 2019-2021 a total of: (i) 26 fines have been applied for failure to submit basic information amounting to € 6 500; 4 companies have been struck off for this reason; (ii) and 15 fines for failure to submit BO information amounting to € 3 750. In both cases average amount of fine is € 250 which is not proportionate in light of greater importance of BO information when compared to basic information. Apart from the fines not being dissuasive, the fact that only 20 % (3) of the total number of fines issued have been settled suggests that regulatory sanctioning regime is not effective.

728. To date, no sanctions have been applied to the existing companies for failure to submit information on the changes of beneficial ownership to the Registry. No cases of provision of false or misleading information to the Registry has been identified to date, thus consequently no sanctions have been applied.

Table 7.2. Sanctions for failure to submit basic information (initial submission and update of information):

	2015	2016	2017	2018	2019	2020	2021 (July)
Number of fines	0	0	0	0	15	10	1
Total value of fines (€)	0	0	0	0	3 750	2 500	250
Percentage of fines settled	0	0	0	0	20	0	0
Criminal sanctions	0	0	0	0	0	0	0
Strike off	0	0	0	0	4	0	0
Other sanctions	0	0	0	0	0	0	0

Table 7.3. Sanctions for failure to submit BO information (newly formed companies):

	2015	2016	2017	2018	2019	2020	2021 (July)
Number of fines	0	0	0	0	10	5	0
Total value of fines (€)	0	0	0	0	2 500	1 250	0
Percentage of fines settled	0	0	0	0	0	0	0
Criminal sanctions	0	0	0	0	0	0	0

Strike off	0	0	0	0	0	0	0
Other sanctions	0	0	0	0	0	0	0

Overall conclusions on IO.5

729. Whilst the more recent reforms to the beneficial ownership regime in Bulgaria are promising, they are severely hampered by both the lack of detailed risk understanding in the country and major implementation issues concerning mechanisms to ensure accurate and up to date beneficial information is available. The failure to take effective action against bearer shares JSCs is also extremely significant.

730. Given the risk and context of Bulgaria and the issues concerning the absence of any fully effective mechanism to ensure that information held on the Registers is accurate is a fundamental deficiency. The AT do not consider that the notary regime in place in Bulgaria is effective in ensuring accuracy of beneficial ownership information then entered onto the Registers. This situation is seriously exacerbated by the fact that during the onsite, the private sector confirmed that their usual source of verification of beneficial ownership was by reference to the Registers. The above concerns, accompanied with major deficiencies relating to bearer shares, nominees and the limited use of effective, proportionate and dissuasive sanctions, are fundamental and thus significantly hamper the basic and BO transparency regime in the country.

731. **Bulgaria is rated as having a low level of effectiveness for IO.5.**

8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

a) Bulgaria to some extent provides timely and generally constructive assistance across the range of requests for international co-operation, including mutual legal assistance (MLA) and extradition. The feedback received from foreign partners is generally positive and shortcomings have only been highlighted in very limited instances. It has been identified, however, that the overly formal national cooperation can delay the timeliness of international cooperation, especially in cases when banking secrecy needs to be lifted for the purpose of execution of an MLA.

b) Bulgaria proactively requests legal assistance. However, due to the significantly high evidentiary standard (especially in ML cases, as identified under Immediate Outcome 7) legal international cooperation is used in all cases with any foreign nexus (e.g., a predicate offence committed, or a company registered abroad, etc.).

c) Extensive duplication of requesting international cooperation has been identified. In many instances a request is made in operational (pre-investigative) proceedings as well as in the investigative (pre-trial) stage with a potential additional overlap by the FID-SANS international requests (also in cases where the case has already been disseminated from, or that do not include FID-SANS dissemination), which can lead to significant prolongation of investigations.

d) Law enforcement agencies (LEAs) seek and engage in both formal and informal cooperation with their counterparts using Europol (SIENA) and Interpol channels. At the prosecutorial level, Eurojust and Joint Investigating Teams (JITs) are also often used, but only to a limited extent in ML cases. With the exception of Financial Supervision Commission (FSC) and Bulgarian National Bank (BNB), supervisors only to some extent proactively seek international cooperation concerning ML/TF issues. The National Revenue Authority (NaRA) and Communications Regulation Commission (CRC) have not yet established international cooperation regarding supervision.

e) Generally, foreign FIUs have provided positive feedback on the quality and timeliness of the information provided by the FID-SANS. In terms of pro-actively requesting FIU information via the channels of Egmont and/or FIU.net, the volume of the FID-SANS outgoing requests has decreased in the recent years due to the very limited human and technical resources of the FID-SANS (i.e., operational analysis).

f) The legal framework for international legal cooperation with European Union (EU) counterparts is comprehensive and without legal or practical obstacles to provide international legal assistance. In relation to non-EU countries some TC deficiencies in minor way might have a negative effect on cooperation.

g) There are case management systems in place for most of the authorities entrusted with coordinating and executing international legal assistance. However, there are no written guidelines (or clear processes established) setting out any type of priorities for

executing requests - a limited level of prioritisation is achieved on a case-by-case basis, based on the personal experience of the authorities working with international legal cooperation. Although in practice it has not yet created major obstacles to provide timely and constructive international legal assistance to foreign counterparts.

h) Bulgarian authorities exchange basic and BO information of legal persons with their international cooperation partners. Although no obstacles in providing the relevant information were identified, the deficiencies identified under Immediate Outcome (IO) 5 can significantly impact the quality of BO information provided.

Recommended Actions

a) All authorities should develop both a clear nation-wide strategy and guidelines (including setting priorities) regarding seeking international assistance (MLA and other forms of international cooperation) in order to ensure systematic, proactive and adequate seeking of foreign assistance in line with the investigative priorities.

b) Bulgaria should significantly enhance the case-management systems already in place, providing for comprehensive data, statistics and other information relevant to the effectiveness and efficiency of the international cooperation within the AML/CFT system for both MLA and other forms of international cooperation. The collected statistics thereof then should be systematically reviewed.

c) LEAs, POs and other authorities involved in investigations should establish a clear procedure for seeking international assistance throughout the procedure stages of a case (from FIU to PO) in order to streamline (avoid subsequent repetition is stages of analysis, pre-investigation and investigation) cases with a foreign nexus (i.e., eliminate the "double" or "triple" requests of assistance).

d) Training should be provided to LEAs providing basic and BO information to foreign counterparts.

732. 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.

8.2. Immediate Outcome 2 (International Cooperation)

8.2.1. Providing constructive and timely MLA and extradition

733. The importance of international cooperation in criminal matters for Bulgaria stems from the geographical location of Bulgaria and the country's ML/TF risk profile. Factors particularly relevant in this field include criminal ML offences related to foreign proceeds where there is a need to prove the criminal origin of the assets abroad as well as the prevalence of predicate offences committed in an essentially trans-national manner, mainly due to the fact that Bulgaria is a part of the Balkan route. The mentioned exposes the country to, e.g., illegal trafficking and trade in drugs, people, arms and both licit and illicit goods particularly by organised crime groups, and other crimes with international nexus.

734. On the basis of various legal arrangements and international legal instruments (including UN, CoE Conventions and EU legal instruments, treaties and other bilateral agreements on MLA, see further Recommendation 36 in the TC Annex), Bulgarian authorities are able to provide a range of assistance in case of requests for international legal cooperation in criminal matters and extradition. The legal framework for international legal cooperation with EU counterparts is comprehensive and without legal or practical obstacles to provide international legal assistance. In relation to non-EU countries some TC deficiencies in minor way might have a negative effect on cooperation. Requests for international legal cooperation and extradition are made and received through the MoJ, the Supreme Cassation PO and the district POs. The exchange of information is carried out by sending and receiving a request for legal assistance directly by e-mail or through the MoJ. MoJ cooperates with the Prosecutors when MLA must be executed or sent. In terms of legal assistance, the vast majority of outgoing requests are sent via MoJ. Also, more than 90% of the MLAs are received through MoJ (no precise statistics are kept).

735. The incoming requests for international legal cooperation in the Supreme Cassation PO are distributed to the prosecutors from the International Department, who have a commitment to take the necessary actions as soon as possible. In the district and regional POs, the distribution of applications is done through a system for random allocation of files and cases. The incoming MLA requests are mainly assigned to investigating prosecutors, who have a commitment to perform the requested actions as soon as possible.

736. There are case management systems in place for most of the authorities entrusted with coordinating and executing international legal assistance with a limited information input into the system and a low level of automation. It is important to stress that there are no written guidelines (nor clear system established within the authorities) setting out any type of priorities for executing incoming MLA requests that would ensure a systematic approach. A limited level of prioritisation is achieved on a case-by-case basis, based on the personal experience of the authorities working with international legal cooperation. Although, in practice non-existence of prioritization mechanisms has not yet created major obstacles to providing timely and constructive MLA to foreign counterparts. As per explanations of competent authorities, resources available to authorities responsible for providing responses to MLA requests and other international legal assistance appear to be sufficient.

737. As per explanations of authorities, the execution of requests for international legal assistance is carried out as soon as possible according to the type of actions required by the foreign state. The execution of legal assistance requests usually takes up to almost 4 months with a maximum period of 6 months (please see Table 8.1 below).

Table 8.1: Incoming MLAs and Extradition Requests on ML

Years	Number of incoming MLAs for ML	Number of incoming ERs for ML	Average time of execution (days)	
			MLA	ER
2015	38	-	171	-
2016	31	3	125	222
2017	44	2	118	37
2018	54	4	156	180
2019	58	-	167	-
2020	64	4	106	22

2021[99]	27	5	24	-

Table 8.2: Incoming MLAs and Extradition Requests (ER) for ML/TF and predicate offences

Offence	2015		2016		2017		2018		2019		2020		2021	
	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER
ML	38		31	3	44	2	54	4	58		64	25	27	5
TF											1			
Participation in an organised criminal group and racketeering	4		2	1	2	1	1				4			
Terrorism				1			3		4					
Trafficking in human beings and migrant smuggling	5	1	11		7		9		6		12	6	4	2
Sexual exploitation, including of children	6		2		6	3	6	2	4	1	2	4	2	1
Illicit trafficking in narcotic drugs and psychotropic substances	3		5		8		2	3	16	1	3	2	4	1
Illicit arms trafficking		1			1		1	1			1			
Illicit trafficking in stolen and other goods									1					
Corruption and bribery			2										3	
Fraud	15		14	1	17		28	3	30	1	45	2	56	14
Counterfeiting currency				1					3		1		1	
Counterfeiting and piracy of products			1		1				1					
Environmental crime					2	1	1		2		1		1	
Murder, grievous bodily injury	1		4		5	3	7		4		5	1	1	
Kidnapping, illegal restraint and hostage-taking							2		1					
Robbery or theft	8	2	13	1	16		11	1	17		17	2	8	1
Smuggling (including in	2		1		2		1				1			

[99]Until June 30

relation to customs and excise duties and taxes)														
Tax crimes (related to direct and indirect taxes)	8		16		22		18		19	1	19	1	6	
Extortion			1		1		1	2		1			1	
Forgery	3	1	1	1	1		2		1		3		6	
Piracy	1													
Insider trading and market manipulation												1		
Total	94	5	104	9	134	10	147	16	167	5	179	44	120	24

738. The most common obstacle for timely execution of MLAs, especially in cases of ML or other financial or economic crimes is the strict application of the banking secrecy provisions. Lifting banking secrecy requires an order approved by a judge, execution of which, together with administrative burden of sending the relevant documents in paper form, can take up to several months based on the practice of authorities responding to foreign MLA request. There are similar issues regarding accessing tax information by certain authorities. In context of MLAs, it should be also stressed that the level of evidence required by Bulgarian courts in ML cases is high (for detailed analysis please refer to IO.7) and there have been instances where information set out in an MLA is considered insufficient for lifting banking secrecy, especially in cases of autonomous or stand-alone ML.

739. In relation to TF, Bulgaria has received only one request for MLA in 2020 (January 15). The request was received from Belgian State Prosecutors Office in relation to an investigation against two persons. One of these persons has been identified to have link to a person being investigated in Bulgaria at pre-trial stage. Bulgaria has executed the received request by providing access to their pre-trial case files, identifying a bank account linked to the suspects and provided information on the account dating from 1 January 2015 to 30 June 2015. Bank account information was provided based on a decision of the Sofia Regional Court from 20 October 2020 to lift banking secrecy.

740. As noted by authorities, in some instances another obstacle for timely execution of international legal requests is the very formal approach to inter-agency communication. All communication is carried out in written paper-based form, exchange of which in many cases significantly prolong the timeliness of a specific task (please also refer to analysis under IO.6 and IO.7). There is a general lack of electronic information exchange system when communicating between state authorities and/or OEs.

741. It should be noted that there have been several different reasons for non–compliance with legal assistance requests identified, e.g., (1) the need for additional information, (2) lack of evidence of a link between a predicate offence and the ML (which is a common practice in the country), but most often (3) practical reasons such as lack of translation, the person not being available in its place of residence. The number of refusals is not significant or disproportionate to

the overall volume of international cooperation – the refusals of executions of MLAs vary from 3 to 8 annually since 2014.[100]

742. With respect to extradition there is a simplified process in place that is applied in cases where the person provides an active agreement before the court for being extradited and waves their right to appeal. In such cases, the person shall be removed from the country within 24 hours, but in practice, it takes more extensive period of time. In cases where the person does not give an active agreement, the decision is subject to appeal and the Court of Appeal decision is final.

743. As described under R.39, Bulgaria's EEAWA specifies the conditions and procedure for effecting extradition to non-EU states, as well as the conditions and procedure for the issuance and execution of EAWs. Bulgaria executes requests for extradition as well as surrender under EAWs generally in a timely manner with some exceptions in relation to simplified process (see description above)).

744. Based on the statistics provided regarding execution of extradition requests, no patterns or trends can be identified nor in ML, nor TF cases (please see Table 8.2). No breakdown of statistics was provided to the AT on which requests are done to EU member states and which to non-EU countries. Also, no comprehensive statistics on successful cases and rejected cases have been provided to the AT.

745. Deficiencies identified under R.39 in regard to dual-criminality requirements for non-EU countries could have a potential impact on effectiveness of international cooperation in relation to extradition for TF. However, in practice, no such cases have been identified.

746. As to conflicts in international legal assistance, the Bulgarian CPC provides for a special procedure for resolving possible jurisdictional conflicts or problems in the presence of an international element in the investigation. With an amendment to the CPC from 2017, a special procedural order is provided for the mentioned. The Bulgarian authorities could not provide an example how these provisions have been used in practice.

747. Feedback from various countries that have requested MLA or other type of international legal assistance from Bulgaria (not exclusively in ML/TF cases) generally indicates an appropriate level of cooperation and good relationship between Bulgarian and counterpart authorities. Although some countries referred to minor problems in case-by-case basis - no trends were identified. Other information provided to the AT including feedback from international partners does not indicate any significant trends or deficiencies regarding quality and completeness of assistance provided by Bulgarian authorities.

748. Assets seized in Bulgaria on behalf of foreign requests technically may eventually be confiscated upon a foreign confiscation order submitted for recognition and execution, but no such action has taken place in practice. For EU member states MLA requests in relation to freezing assets is executed in accordance with Art. 8 of the Recognition, Execution and Transmission of Confiscation and Seizure Orders and Decisions Imposing Financial Penalties Act 2010. No statistics have been provided to the AT on the number of executed freezing orders in order to conclude that it is done in an effective manner. However, no negative international cooperation feedback has either been received in relation to Bulgaria's capacity of executing such freezing orders (for a successful execution of foreign freezing order see case example below).

[100] 2014 – 3, 2015 – 8, 2016 – 7, 2017 – 7, 2018 – 4, 2019 -3, 2020 – 6, 2021 (until June) - 1

Box 8.1: Case example of executing foreign asset freezing order (year 2019)

At the request of the District Court in the city of Leipzig, proceedings were instituted before the Sofia City Court under Art. 8 of the Law for recognition, execution and enactment of acts for securing property or evidence. This was in connection with proceedings in case of fraud against the financial interests of the European Community and computer crime, the PO in Germany sent an MLA request to the Sofia City Prosecutor's Office (SCPO) to secure bank assets for future seizure. The SCPO sent a procedural order No. 1135/20.03.2019 to the Sofia City Court (SCC) requesting to freeze 310,000 EUR of bank assets according to article 3 of the Recognition, Execution and Enactment of Freezing Injunctions Act. On March 20, 20219, the court issued a decision recognizing and enforcing the act of securing property. The court has ordered the property to be kept in the Republic of Bulgaria for the purpose of subsequent confiscation. A precautionary order was issued on the same day and sent to a state bailiff. According to the information received (in court) by the bailiff, the first seizure was actually imposed on March 21, the second on March 22, and the third on March 25 of year 2019.

The time for execution of the foreign court decision is about two weeks - it was received by the prosecutor's office on March 7, 2019, and the actual seizure of the accounts took place in the period March 21-25, 2019.

749. Foreign confiscation orders can be executed in Bulgaria through the general mechanism applicable for recognition and enforcement of foreign court decisions, provided that there is a bilateral or multilateral treaty basis and that the foreign judgment, which pronounced the confiscation measure, has previously been recognized by a domestic court order.

750. In relation to EU member states, foreign confiscation orders are recognized and executed in a certificate mechanism introduced by Council Framework Decision 2006/783/JHA (implemented by Recognition, Execution and Transmission of Confiscation and Seizure Orders and Decisions Imposing Financial Penalties Act 2010). The District Courts are authority for receiving and sending of certificates of confiscation orders and in course of the proceedings communicate directly with the judicial authorities of member states. In case it is not possible to establish direct contact between the courts, the correspondence should be addressed to MoJ. From the examples of executed confiscation orders the AT has concerns on the timeliness of the assistance provided by Bulgaria. In average it takes up to 6 months to enforce a confiscation order from EU and non-EU jurisdictions. Moreover, case examples provided by Bulgaria indicate that in practice competent authorities have not executed foreign confiscation request when 'the act for confiscation was taken in absentia'.

751. The information and statistics provided to the AT refers to the time period of 2020 and 2021, therefore it cannot be concluded that Bulgaria executes incoming MLA requests in relation to freezing, seizure and confiscation in a systemic way.

752. No information was provided to the AT on the value of assets seized upon foreign requests, the value of assets returned (by means of repatriation, restitution, or sharing of assets), nor information on any practice in sharing of confiscated assets with other countries. The issues identified under IO.8 in relation to asset management are also relevant in context of international cooperation.

8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

753. In all cases in which evidence must be collected or actions must be taken in a country outside Bulgaria, prosecutors and investigative bodies shall prepare and send a request for international legal assistance. Requests for international legal cooperation shall be made by the supervising prosecutors together with the investigative bodies designated in the relevant pre-trial proceedings.

754. Outgoing requests are prioritized in a similar manner as incoming, namely, a limited level of prioritization is achieved on a case-by-case basis, based on the personal experience of the authorities working with international legal cooperation. If there is a clear deadline for an outgoing request the MoJ (central authority also for outgoing international legal assistance) is in practice notified by PO in advance in order to meet the relevant deadline.

755. There are no written guidelines (or clear processes established within relevant authorities) setting out any type of priorities for requesting international legal assistance. Although a level of prioritising is achieved on case-by-case basis, this is considered to be a major deficiency which to a very large extent impedes requesting international assistance in ML cases. A major problem is the fact that requesting international assistance is duplicated or even triplicated during the course of working on a case, especially, in cases when FID-SANS channels are used repeatedly after information has already been disseminated from the FID-SANS or cases without FID-SANS disseminations (i.e., LEAs in some instances revert to the FID-SANS for requesting information via international information exchange channels). In practice, international assistance is requested in the operational or (pre-investigative) stage and then the same information is requested in the investigative or (pre-trail) stage due to the fact that information collected in the operational or pre-investigative stage cannot be used as evidence (as discussed above under IO.7). In cases where information is disseminated from the FID-SANS, the international assistance is also requested in that stage (via ESW of FIU.net channels). Authorities explained that this is a common practice and requesting information in the operational stage is requested by the POs. Authorities additionally indicated that requesting information via FID-SANS channels is used in cases where there is not enough information to request MLA.

Box 8.2: Outgoing and incoming MLA on ML (complex cross-border investigation)

Initially, a file was opened in the Regional PO on materials sent by the Directorate of FID-SANS, and then sent by competence to District PO.

In the case it was established that the accused opened a bank account in Bulgaria. The individual was Romanian citizen. He stated that he would receive remittances from abroad. Only he had the right to operate the account. During the period 12.12.2012 – 21.12.2012 a total of seven bank transfers, received by various individuals from Spain, were received on this account. The sums received were immediately withdrawn in person by the accused, in cash. The total amount of money thus obtained amounted to EUR 2,100. Shortly afterwards it was reported that the transfer was made due to fraud committed on the Internet (goods were ordered and paid for but not delivered) and with a request for cancellation. The predicate offence under Art. 209(1) in conjunction with Art. 26(1) of the Penal Code was fraud committed through the Internet. The property damage amounts to a total of 2,100 EUR. The predicate offence was committed in Spain and is investigated by the competent judicial authorities in Spain and is not part of the present criminal proceedings.

In this case, Bulgarian authorities sent to two MLA requests to Spain and Romania. As a result, no expert reports were pointed in the case and no material evidence was seized. There is no secured property in the case. No bank accounts were blocked in the present case.

756. It should be stressed that the general approach of the country is to request international assistance in almost every case when pursuing domestic ML with suspicion of predicate offence potentially being committed abroad or with any other foreign nexus, e.g., a company registered abroad (please see case example above in Box 8.3). As explained by the PO this is done to meet the evidentiary burden of proving predicate offence. Authorities also noted that the pre-investigative as well as the pre-trail stage are significantly prolonged due to the fact that the answers for requested international assistance are not always provided in a timely manner by foreign counterparts. Especially, this is an issue in cases of requests to offshore jurisdictions. The AT fully agrees with the effect that the over-requesting of international assistance has on the timeliness of investigations identified by the authorities.

Table 8.3: Number of outgoing MLAs and Extradition Requests (ER) for ML/TF and predicate offences

Offence	2015		2016		2017		2018		2019		2020		2021	
	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER	MLA	ER
ML	30		21		22		33	3	42	5	38		31	10
TF									1					
Participation in an organised criminal group and racketeering			1	1										
Terrorism	2								2					
Trafficking in human beings and migrant smuggling	8		6		13		24		15		8	0	2	0
Sexual exploitation, including of children					1				1				1	0
Illicit trafficking in narcotic drugs and psychotropic substances	3		2		2		5		4					
Illicit arms trafficking														
Illicit trafficking in stolen and other goods									1					
Corruption and bribery	8		2		1		1		3		8	0	4	0
Fraud	2		27		45		50	1	73		39	7	18	1
Counterfeiting currency			1				1		3		1	0	2	0
Counterfeiting and piracy of products	1								2		3	0	3	0

Environmental crime					2			1			1	0		
Murder, grievous bodily injury	10		8		5		6		9		4	0	2	0
Kidnapping, illegal restraint and hostage-taking					1				1		1	0		
Robbery or theft	8		10	1	21		23		13		12	0	8	0
Smuggling (including in relation to customs and excise duties and taxes)											2	0		
Tax crimes (related to direct and indirect taxes)	29		4		10		8	2	21		21	3	5	0
Extortion	1													
Forgery	1		1		7		3		9		4	0	2	0
Piracy														
Insider trading and market manipulation														
Total	74	-	67	2	93	-	113	7	131	1	142	10	78	11

757. The described process of requesting international legal assistance, however, does not necessarily appear to be substantiated by the statistics. When looking at the Table 8.3 above, the number of MLAs requested in ML cases (217 requests between 2015-2021), appears to be moderate when considering the ML risk exposure and geographic location of Bulgaria. Perhaps, this can be explained with rather small number of domestic ML investigations, and as noted under IO.7 is not in line with countries risk profile. In regard to the assistance being sought in line with the countries` ML/TF risk profile, analysis under IO. 6 and IO 7 should be taken into account (e.g., the high number of ML cases concerning various forms of fraud does not fully cover the country's ML/TF risk profile). Also, the feedback provided by Bulgaria's international partners indicates that most of assistance is sough regarding fraud and tax crimes. No specific trends can be identified regarding volumes of outgoing extradition requests (please see Table 8.3).

758. In relation to requesting MLA from foreign counterparts for seizure and confiscation of assets in ML related cases during the period under review, the AT was not provided information if this has ever occurred in practice.

759. Over the time period under consideration Bulgaria has made 18 requests for extradition with respect to ML (see Table 8.3). No information was provided to the AT whether these requests have been executed. There were no occasions for requesting extradition for TF.

8.2.3. Seeking and providing other forms of international cooperation for AML/CFT purposes

760. There is a number of international co-operation mechanisms and arrangements with other countries in place in the fields of financial intelligence, supervision and law enforcement. These including bilateral and multilateral MOUs, treaties, co-operation based on reciprocity, or other co-operation mechanisms.

FID-SANS

761. The FID-SANS has all the instruments in place to provide financial intelligence and additional information to requesting foreign FIUs. When engaging in international cooperation the FID-SANS has all the powers to obtain, analyse and provide information as with the operational analysis triggered domestically (based on STRs from obliged entities, information from state bodies, etc.).

762. The FID-SANS has signed MoUs with 33 foreign FIUs, although an existence of a signed MoU is not a mandatory requirement for international information exchange. Art.90 (1) of LMML and Art. 14(2) of LMFT provides a broad legal basis for exchange of information. According to it the FID-SANS can exchange information with the relevant foreign authorities based on reciprocity regardless of the existence of cooperation agreement or MoU, as well as not only with foreign FIUs but also with other competent authorities when it comes to prevention and combating ML, associated predicate offences and TF.

763. Also, the FID-SANS exchanges information with non-counterparts through diagonal cooperation. Many of the incoming requests from foreign FIUs are made on behalf of the LEAs of the particular country. There are no limitations for the FID-SANS in providing comprehensive replies to such requests (please see case example below).

Box 8.3: requests from foreign FIUs are made on behalf of the LEAs (year 2018)

FID-SANS received request from the foreign FIU which was supporting an investigation of their LEAs on organized criminal group with leader – foreign national involved in the production of narcotic drugs for their further trafficking. The investigation revealed that money remittances and bank transfers were conducted between the foreign country and Bulgaria by the main suspect and related persons.

This request was received in 2018 and initial reply was provided within 13 days from receiving the request. FID-SANS initially informed its foreign counterpart on the results from the FIU databases checks, incl. searches in the police border control database which established that the a.m. foreign national crossed Bulgarian borders in multiple times and in many of these occasions the suspect was travelling with Bulgarian national who is involved in several Bulgarian companies together with the foreign national. Additional correspondence was held subsequently between FID-SANS and the foreign FIU based on the collected additional bank information and the conducted additional checks. Checks on the Bulgarian national for criminal records showed that latter was previously arrested and sentenced to imprisonment for possession of narcotic drugs without permission (conditional sentence). FID-SANS obtained full bank information on the involved subjects from the Bulgarian commercial banks. The information obtained on all concerned accounts revealed that the foreign national transferred funds from accounts in his country to his accounts in Bulgaria, as well as to Bulgarian company and the funds were subsequently withdrawn in cash (either at cash desk or ATM) by the foreign

national or the a.m. Bulgarian national who was proxy on the accounts. Several transactions through money remitters were also identified. FID-SANS provided the foreign FIU with analysis on the collected information with detailed description on the conducted transactions with the respective consent to the foreign country LEAs.

As explained by the FID-SANS, the acquired data enabled the foreign FIU and LEAs to ascertain precisely the role of each organized criminal group member, to finalize the legal assessment of the subjects' activity and to extradite the foreign national to his country.

764. The exchange of information of the FID-SANS with foreign FIUs takes place through secure channels – ESW and FIU.net. As per information safeguards in place - the ESW and FIU.net points of access are 3 computer stations (1 for ESW) and (2 for FIU.Net) which are used only for the purposes of exchange of information. The information units sent or received through ESW and FIU.net are printed and/or recorded on CDs (depending on the volume) which are registered in the Registrar Office of the FID-SANS and assigned for processing to the analysts. For each request/spontaneous disclosure a separate file is opened where the documents received and produced on the case are kept (incl. numbering and listing). The printed or CD materials are stored in a special archive where access is given only with the necessary clearance level.

765. The priority of incoming requests is assigned by the head of the relevant sector in charge of international cooperation on case-to-case basis. There are no guidelines or prioritization documents in place for incoming or outgoing international cooperation documents. It should be noted that FID-SANS does not keep statistics on the timeliness of the responses to or from its counterparts. The FID-SANS efforts are aimed at providing the information within 14-30 days of the receipt of routine request.

Table 8.4: FIU to FIU cooperation[101]

	2015	**2016**	**2017**	**2018**	**2019**	**2020**	**2021[102]**
INCOMING REQUESTS							
Foreign requests received by the FIU	180	155	198	303	354	362	191
Foreign requests executed by the FIU[1]	207	206	226	331	370	349	168
Foreign requests refused by the FIU	0	0	0	0	0	0	0
Spontaneous sharing of information received by the FIU	56	73	98	146	150	127	106
TOTAL (incoming requests and information)	236	228	296	449	504	489	297
Average number of days to respond to requests from foreign FIUs	Not available	Not available	Not available	Not available	Not available	Not available	Not available
Refusal grounds applied	-	-	-	-	-	-	

[101]The figures include executed requests from the previous years too, e.g., if these were received at the end of the previous year. Thus, in 2014 10 requests from December 2013 were executed. The figures for the period 2015 – 2019 also include limited number of feedbacks sent to foreign FIUs on some of their spontaneous disclosures. FID-SANS does not send feedbacks to all spontaneous disclosures, but only when the checks in FID-SANS databases have revealed information that is considered be potentially of interest to the foreign FIU.

[102]Until 31.07.2021

OUTGOING REQUESTS							
Requests sent by the FIU	240	184	155	157	149	134	99
Spontaneous sharing of information sent by the FIU	2	6	17	93	77	51	17
TOTAL (outgoing requests and information)	242	190	172	250	226	185	116

766. As set out in the table above, there is significant increase in foreign FIU requests in the recent years (especially since 2018). However, the trend in the volumes of outgoing requests is the opposite, where a noticeable decrease can be observed since 2015. As per explanations of the FID-SANS, this is mainly due to the general lack of resources of other departments of FID-SANS (for more information, please refer to information under IO.6). FID-SANS noted that at the time of the on-site additional staff would be helpful also for the needs of exercising international cooperation.[103]

767. In terms of freezing upon request, FID-SANS informed that since 2018 unknown number of requests for freezing have been received and in 3 cases FID-SANS has exercised its powers to postpone transactions. Although, FID-SANS does not hold powers to freeze assets, it has the possibility to postpone transaction (for more detailed explanation, please refer to IO.6). In cases of foreign requests, the FID-SANS exercises this power in conjunction with the power to monitor accounts as demonstrated in the case example below. In all 3 of these cases, this mechanism was applied.

Box 8.4: Case example demonstrating successful FIU to FIU cooperation

Partner FIU approached FID-SANS with urgent request regarding a fraudulent transfer approximately for 50 000 EUR from their country to local account of Bulgarian company (owned and managed by foreign national). The funds were credited on the account on the same date as of the date of receipt of the request on the basis of CEO fraud. FID-SANS was requested to block the funds, if possible, until MLA request was prepared and sent to the competent authorities in Bulgaria. The performed checks established that the fraudulent transfer was reported in STR and the funds were still available on the account. FID-SANS further instructed the bank to place the account under monitoring and to report to FID-SANS on any attempt for disposal actions with the funds so that the Head of the Bulgarian FIU could exercise its powers to postpone a transaction. The information on the current status of the account and on the initiated actions by FID-SANS was provided to the foreign FIU on the next day of the day of receipt of their request.

768. Generally, foreign FIUs have provided positive feedback on the quality and timeliness of the information provided by the FID-SANS. However, in terms of pro-actively requesting FIU information via the channels of ESW and FIU.net, the volume of the FID-SANS outgoing requests has decreased in the recent years due to the very limited human and technical resources of the FID-SANS (i.e., limited operational analysis).

Supervisory institutions

769. No comprehensive statistics have been provided by the FID-SANS regarding cooperation on international information exchange as a supervisor (apart from indication that 9 requests have been made in 2021), therefore it seems that whilst FID-SANS to some extent cooperates with the

[103] As explained by the FID-SANS, 2 such staff members will be on-boarded and at the time of the on-site is already in the process of being hired and allocated to international cooperation department).

competent authorities of third countries regarding ML/TF it does not do so regarding supervision matters even despite the fact that some of the supervised entities are forming part of international groups.

770. The BNB is signatory to more than 20 multilateral and bilateral MoUs. The BNB has received a total 39 and sent a total 23 requests during the reporting period. The average time taken for the BNB to respond varies from 3 days for a simple request to 3 months in cases where the foreign counterpart raised an ML/TF concern that prompted inspection by the BNB.

Table 8.5: BNB Foreign Cooperation requests (incoming/outgoing)

Incoming	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**31.07.21**
Requests received	1	9	8	7	1	6	7
Requests executed	1	9	8	7	1	6	7
Requests refused	0	0	0	0	0	0	0
Average execution time (days)	10	10/90	10/90	10/90	10	4/90	3/20
Outgoing	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**31.07.21**
Requests sent	0	0	2	0	3	13	5
Requests executed	0	0	2	0	3	13	5
Requests refused	0	0	0	0	0	0	0

771. The FSC is signatory to more than 70 multilateral and bilateral MoUs. The FSC has received a total 111 and sent a total 96 requests during the reporting period. The average time taken for the FSC to respond to a request is 30 days. There have been no instances of refusal of a request received or sent by the FSC. During the onsite, the evaluators were advised that cooperation requests are typically made under the IOSCO MoU and relate to ML/TF investigations, potential inspections and concerns over the owners and controllers of licensed entities.

Table 8.6: FSC Foreign Cooperation (incoming/outgoing)

Incoming	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**31.07.21**
Requests received	2	5	17	38	28	21	-
Requests executed	2	5	17	38	28	21	-
Requests refused	0	0	0	0	0	0	-
Average execution time (days)	30	30	30	30	30	30	-
Outgoing	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**31.07.21**
Requests sent	8	5	20	5	35	23	-
Requests executed	8	5	20	5	35	23	-

Requests refused	0	0	0	0	0	0	-

Table 8.7: FSC Cooperation regarding entry controls

Cooperation type			2017	2018	2019	2020
Requested - Fit and proper			3	4	29	6
Responded - Fit and proper			2	4	4	3
Requested - Beneficial ownership			9	3	7	4
Responded - Beneficial ownership			0	5	5	3

772. Other supervisors, namely the NaRA regarding currency exchange and gambling and the Communications Regulation Commission (CRC) have not established any agreements for cooperation with foreign counterparts.

773. The absence of foreign cooperation is particularly concerning regarding online gambling as the NaRA currently licences entities that form part of groups that are licenced in other jurisdictions, including a jurisdiction identified by the FATF as having strategic weaknesses in AML/CFT.

774. Agreements may have been established by the former gambling supervisor, the State Commission on Gambling (SGC), however no information or statistics are held by the NaRA regarding the activities of the SGC undertaken prior to its abolishment in 2020 (for more information, please refer to IO.3).

LEAs

775. International Operational Cooperation Directorate (IOCD) of the MoI is the competent authority responsible for organisation and co-ordination of law-enforcement informational exchange. The IOCD is the national contact point in the context of the INTERPOL, EUROPOL, ETIAS and the SIS and fulfil the commitments of the Republic of Bulgaria as National Central Bureau INTERPOL, Europol National Unit, ETIAS National Unit and SIRENE Bureau. The IOCD is also responsible for bilateral information exchange via liaison officers' network under the concluded bilateral agreements for police cooperation.

776. The IOCD manage and monitor all channels for information exchange in 24/7 regime. The IOCD is a Single Point of Contact where the core law-enforcement information channels are based and available. The information is prioritized, processed and provided to the national authorities according to their competencies.

777. All national LEAs (MoI, SANS, ARO, National Customs Agency, judicial authorities) can exchange information with their counterparts through IOCD and *vice versa*.

778. A practice implemented by the IOCD is the practice of so-called "first response". When request is received, IOCD officers carry out checks in all available to the Directorate databases, which are part of databases of MoI and send the results to the requesting partner. All the bases are safe and the information in them is official. After then the request, together with the results

of the initial checks, are forwarded to the relevant national competent authority for notification and for further checks.

Table 8.8: Law enforcement cooperation

International co-operation	2015		2016		2017		2018		2019		2021		2021[104]	
INCOMING REQUESTS	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Foreign requests received by law enforcement authorities related to ML/TF	1 Pers. * 56**	8 Pers. *	10 Pers. * 100**	3 Pers. *	6 Pers. * 101**	1 Pers. *	2 Pers. * 215**	0 Pers. *	0 Pers. * 466**	0 Pers. *	3 Pers. * 261** 108***	0 Pers. * 2	3 Pers. * 160** 56***	0 Pers. * 1
OUTGOING REQUESTS	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Number of requests sent abroad by law enforcement authorities related to ML/TF	29**		43**		60**		71**		111**		45** 212***		36** 110***	
Number of requests sent and executed							20***		40***					
Number of requests sent and refused							0***		0***					

* Number of investigated persons for terrorism, and the number of extradited/transferred persons upon EAW, investigated for money laundering. This statistical information represents the number of investigations and exchange messages via SIRENE Bureau.
** Number of request of investigations via Europol SIENA.
*** Number of investigations and exchange messages via INTERPOL.

Table 8.9: JITs (Joint Investigation Teams) for the period from 2014 to the present

Year	Number and topic of JITs
2015	3 JITs were concluded, and the subject was predicate offences – OCG, human trafficking, computer abuse, extortion, theft and ML. They have been established with the competent authorities of the following countries – 1 with Great Britain, 1 with the Kingdom of the Netherlands, 1 multinational (Romania, Lithuania, Moldova, Europol and OLAF).
2016	1 JIT with the Kingdom of Spain – for OCGs, trafficking in human beings for the purpose of sexual exploitation and ML
2017	1 JIT with the Republic of France – for OCGs, trafficking in human beings for the purpose of sexual exploitation and ML
2018	1 JIT with United Kingdom – for OCG, trafficking in human beings for sexual exploitation and ML
2019	-
2020	1 JIT with the Republic of Italy – for ML. The case is still pending before the Specialised Prosecutors' Office

[104] Until 31 July 2021.

Box 8.5: Case example demonstrating the usage of joint investigation team

Trafficking in human beings took place in the Kingdom of Belgium and the Kingdom of the Netherlands.

In the course of the investigation, a joint investigation team (JIT) was set up with the investigating authorities of the two countries – the Kingdoms of Belgium and the Netherlands, in order to gather evidence of criminal activity in their territory on trafficking in human beings by Bulgarian citizens. activity under Article 321 of the Penal Code in the Republic of Bulgaria, the discussed pre–trial proceedings were instituted.

With the signed agreement on the establishment of the JIT between the participating countries it was agreed, in addition to the exchange of information and evidence gathered, the investigation to be divided, and the authorities of the Kingdom of Belgium and the Netherlands to prosecute criminal activity in human trafficking, and the investigative bodies of the Republic of Bulgaria to engage in criminal activity under Article 321 of the Penal Code – organized criminal group and money laundering under Article 253 et seq. of the Bulgarian Penal Code.

In the course of the investigation in Bulgaria, data were requested in accordance with the ECA, after the respective sanction – permission of the Specialized Criminal Court (Specialised Criminal Court). An analysis of the data received from mobile operators was performed. Requests for the use of SIM have been prepared and such permits have been issued by the Specialised Criminal Court. Subsequently, with the permission of a judge from the Specialised Criminal Court, investigative actions were carried out – inspections, searches and seizures, through which material evidence was collected, incriminating specific persons for specific criminal acts. In the meantime, many people were questioned as witnesses, incl. and trafficked individuals who identified future defendants.

The investigating authorities have requested from the Municipality of Sliven and the Directorate for National Construction Control documents certifying a construction permit and a construction line, time for started and completed construction, commissioning, as well as for identification of the investor and contractor of buildings in four plots of land in the area of Sliven.

779. There have been 6 JITs established based on the initiative of the Bulgaria's investigative bodies since 2015.

780. The Republic of Bulgaria, represented by the CACIAF is a part of ARO Platform, as well as has been a full member of the CARIN network since 2007. The CACIAF is a partner institution in the SIENA Program which is a system for the exchange of operational and strategic information between EU Member States, Europol and third countries.

781. Other competent specialized directorates of SANS commence international information exchange mainly through liaison officers. Also, on operational level the international cooperation is provided through data exchange with the police liaison officers and the SIENA channel of Europol, as Interpol as well. SANS has national contact points in the international operational networks CARIN and AMON. Inquiries on behalf of foreign counterparts and exchange with their foreign counter parts are conducted under European Investigation Order with the supervision of the competent PO.

Table 8.10: Requests for assistance received in SANS

Requests for assistance received in SANS from:					
	2014 -2018	**2019**	**2020**	**2021**	**Total**
Bundescriminalamt - Germany	301	5	31		337
Austrian Police Attaché		1	1		2
FrenchPolice Attaché	141	2	9		152
French Customs Attaché		3	3		6
FBI	41	3	1		45
Other		3	5		8
NCA/SOCA	32	2	2		36
HMRC		8	2		10

Table 8.11: Correspondence sent by SANS

Correspondence sent by SANS to:					
	2014- 2018	2019	2020	2021	Total
Bundescriminalamt - Germany	137	8	18		163
Austrian Police Attaché		1	1		2
French Police Attaché	149	1	1		151
French Customs Attaché		2	2		4
FBI	35	23	6		64
Other		1	2		3
NCA/SOCA	69	1	1		71
HMRC		2	1		3

8.2.4. International exchange of basic and beneficial ownership information of legal persons and arrangements

782. Generally, there are no obstacles for the competent authorities to exchange of BO information with their foreign counterparts. There are no legal impediments and in most of the requests sent and received such information is being sought and provided from and to the requested and requesting foreign counterpart.

783. Supervisors (e.g., the BNB) confirm that as regard to received requests from foreign competent authorities they provide information, based on information from Bulgarian Commercial register.

784. The FID-SANS regularly provides and seeks basic and BO information; however, no exact statistics could be provided by the country on this matter. Usually, this information (basic and BO information) is integral part of most information requests of both the foreign FIUs and the FID-SANS in addition to STRs, criminal records and other financial information. Requests that seek solely basic and BO information are very rare. There were no cases identified in the practice of the FID-SANS, where the BO information provided to foreign counterpart was different from the information held in the Commercial Register, despite the fact that usage of "straw-man" is one of the most common typologies in Bulgaria. The FID-SANS has, however, provided examples with replies to foreign requests with an indication that "the owner of a company could potentially be (or is) a straw-man".

785. The FID-SANS is making use of the BO information through a direct access to Commercial Register, available STRs, as well as its powers to request information from OEs. Even before the establishment of the BO register, in the cases where foreign company appeared as owner of Bulgarian entity in the records of the Commercial Register, the FID-SANS obtained the BO information from OEs (mainly banks). This is a major deficiency in conjunction with other deficiencies identified under IO.5, which can impede effective exchange of basic and BO information with the foreign counterparts.

Overall conclusion on IO.2

786. Bulgaria provides to some extent timely and generally constructive assistance across the range of requests for international co-operation, including MLA and extradition. The feedback received from the foreign partners is generally positive and shortcomings have only been highlighted in very limited instances. However, the overly formal national cooperation can delay the timeliness of international cooperation, especially in cases when banking secrecy and tax information secrecy needs to be lifted for the purpose of execution of an MLA.

787. Bulgaria to some extent proactively requests legal assistance and other forms of international co-operation. However, due to the very high evidentiary standard in ML cases (please see IO.7.) international cooperation is used in almost all cases with any foreign nexus (e.g., a predicate offence committed, or a company registered abroad, etc.). In such cases, not always commensurate and adequate assistance is sought.

788. Extensive duplication of requesting international cooperation has been identified, where a request is made in operational stage and in the investigative stage with a potential additional overlap by the FID-SANS international requests (including, in stages where information has already been disseminated from the FID-SANS or in cases without any FID-SANS disseminations). The volume of MLAs requested in ML cases, appears to be moderate when taking into account the ML risk exposure and geographic location of Bulgaria.

789. LEAs seek and engage in also informal cooperation with their counterparts using Europol (SIENA) and Interpol channels. At the prosecutorial level, Eurojust and JITs are also often used, but only to a limited extent in ML cases. With the exception of FSC and BNB, supervisors would benefit from more proactively seeking international cooperation concerning ML/TF issues. The NaRA and CRC have not yet established international cooperation regarding supervision Basic and BO information of legal persons is exchanged with international cooperation partners. Although no obstacles in providing the relevant information were identified, the deficiencies identified under IO.5 can significantly impact the quality of BO information provided.

790. The AT notes that absence of quantitative information (statistics) and relevant qualitative information (case studies) is a significant deficiency identified also in regard to international cooperation. For this reason, Bulgaria could demonstrate the effectiveness of their international cooperation to some extent and the AT concludes that major improvements are needed.

791. **Bulgaria is rated as having a moderate level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations in 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.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2013. This report is available from Bulgaria (coe.int).

Recommendation 1 – Assessing risks and applying a risk-based approach

Risk assessment

Criterion 1.1 – Art. 95 of the Law on Measures against Money Laundering (LMML) and Art. 59 of the Rules on Implementation of the Law on Measures against Money Laundering (RILMML) requires Bulgaria to perform a national risk assessment of money laundering and the financing of terrorism to identify, assess, understand and mitigate the risks for the purposes of the LMML and of the Measures against the Financing of Terrorism Act (MFTA).

Art. 96 of the LMML provides for the designation of competent authorities through a standing interdepartmental working group and provides them powers to request information both from the public and private sector, while Art. 97 of the LMML and Art. 59 of the RILMML provide for follow-up actions.

The first holistic national risk assessment of money laundering and the financing of terrorism was finalised in November 2019 (NRA). The adopted NRA report analyses the internal and external ML and TF risks that the country faces. The Bulgarian authorities used the CoE's NRA methodology.

The NRA report has produced a matrix or risk scenarios for Bulgaria which have been compiled into a series of top-level ML risk events in the Executive Summary of the report. The risk assessment demonstrates a general understanding by Bulgaria of the risks that it faces and particularly notes the high level of risk presented by the widespread use of cash (leading to the risk of a significant shadow economy), identified levels of corruption and activities of organised crime groups.

However, ML events covered in the NRA are generic and whilst there is analysis of inherent threat factors, it is not clear how the residual risk has been arrived at in the NRA. There are also deficiencies in the risk assessment data in respect of the threats emanating from corruption, domestic PEPs and non-resident PEPs specifically linked to the investment-related residence and citizenship (IRRC) programme.

Initial steps were taken by the authorities in the NRA report to understand the risks the VASP sector may pose in terms of ML/TF. However, there has not yet been a full assessment of the VASPs sector or emerging products conducted by Bulgaria (see also c.15.3).

Between 2014-2017 a variety of sector specific reports were conducted by the BNB - SSAD who had performed annual risk assessments of the ML/TF risk of credit institutions which operate on the Bulgarian market on the basis of information received by the BNB.

With respect to the NPO sector, Bulgaria has not conducted any comprehensive analysis of NPO sector recently (last analysis was conducted in 2012) (see also c.8.1). The NRA and the risk events

did, however, reflect the Bulgarian NPO sector with medium risk, based on observations and Bulgarian context in the period 2016-2019.

Overall, the risk assessment does not yet demonstrate a good understanding of the residual ML/TF risks faced by Bulgaria however, work conducted so far generally identifies and assesses ML/TF risks to some extent.

Criterion 1.2 – Art. 96(1) of the LMML established a standing interdepartmental working group which is empowered with powers under the same statute. The Interagency Working Group on National Risk Assessment and Management (NRAM WG) was established according to Art. 96 (2) with Council of Ministers Decision as a body that serves as the ultimate decision making and oversight body of the NRA process and risk management. This working group can be considered as a successor of the previously established ad-hoc working group, which was established with the joint Ordinance of the Minister of Interior and the Chairperson of the SANS.

Criterion 1.3 – Art. 95(1) of the LMML requires for the NRA to be updated every two years.

Criterion 1.4 – Art. 97(2) of the LMML requires Bulgaria to make the results of the national risk assessment and its updates available to FIs and DNFBPs but also states that a summary of the risk assessment which does not contain classified information shall be published on the website of the State Agency for National Security. Information on the NRA was published at the official websites of the SANS[105] and FSC[106] in order to inform OEs under its supervision. Equally results of the NRA have been published on the internal website of the Prosecutor's Office (PO), available to all prosecutors and investigators in Bulgaria.

The AT consider that whilst the results have been published to some extent, the publication is limited in terms of content and does not reflect in detail the conclusions of the NRA.

Art. 96(3) and (4) of the LMML also provides for the high level of involvement of the competent authorities in the whole NRA process which includes providing information on the results of the NRA process on their websites. Despite the more limited publication of the NRA documentation, the authorities have conducted a number of sector specific meetings, trainings and have sent letters which look to explain in more detail the conclusions of the NRA.

Criterion 1.5 – This criterion's requirement is addressed in Art. 97(1) and in Art. 96 (1) of the LMML as well as in the general requirement to conduct NRA of Art. 95 of the same law.

Whilst Art. 96 (1) of the LMML establishes the working group that carries out and reports on the results of the NRA along with proposals in an action plan for mitigating risks the LMLL does not refer specifically to the application of resources and implementing measures to prevent or mitigate ML/TF.

Art. 97(1) of the LMML requires that the results of the NRA shall be used to improve the regime of the prevention and countering of money laundering and terrorist financing and notably Art. 97(1)3. of the LMML specifies that the results should be used to allocate and prioritise means and resources to counter ML/TF. However, this does not explicitly state that resources should be applied considering a risk-based approach across all relevant agencies.

[105] https://www.dans.bg/en/msip-091209-menu-en/results-from-national-risk-assessment
[106] https://www.fsc.bg/bg/normativna-uredba/merki-sreshtu-izpiraneto-na-pari/natsionalna-otsenka-na-riska-ot-izpirane-na-pari-i-finansirane-na-terorizma-v-republika-balgariya/

Art.114 of the LMML specifically requires that the "*control activities regarding the application of measures for the prevention of use of the financial system for the purposes of ML shall be carried out by applying a risk-based approach*" – which is then defined as including, amongst other factors, information relevant to the assessment of ML risk in the NRA process.

The requirement also applies for TF risk Article where Art. 14a of the LMFT states that control over compliance with the obligations under LMFT by the persons referred to in Article 4 of the LMML (OEs) shall be exercised according to the procedure established by Chapter Nine of the LMML. Art. 114 of the LMML is in Chapter nine of the LMML which applies the assessment to TF risk. TF risk is also covered in Art. 114, para 1, item 2 of the LMML – "*use of the information collected to assess and understand the risk of money laundering and financing of terrorism to which the persons referred to in Article 4 herein are exposed, as well as the measures taken by the said persons to reduce and mitigate the said risk*;"

Art. 115 of the LMML requires FID-SANS, the BNB, the FSC and NaRA to identify the risk when carrying out inspections. In practice this therefore applies a RBA to the allocation of supervision resources in Bulgaria.

Arts. 95 – 97 of the LMML require allocation of resources, to some extent, at a national level. This includes the allocation of human, technical, financial and any other type of resources.

Resources have been allocated to the Action Plan post its adoption by the Council of Ministers on 16th September 2021, however, the AT do not consider the resources are sufficient to deal with the significant actions assigned to the NRAM WG.

Article 97(1), items 6 and 7 of the LMML also envisage the publication of reports on resources.

Criterion 1.6

(a) Exemptions are envisaged with regard to e-money, pursuant to Art. 24 of the LMML and respectively Art. 34 of the RILMML, which transpose the Art. 12 of Directive (EU) 2015/849 of the European Parliament and of the Council (4th AMLD) and its amendments with Directive (EU) 2018/843 of the European Parliament and of the Council (5th AMLD). Art. 24(1) of the LMML provides an exemption for e-money issuers and their representatives and can be applied to limit the application of certain CDD measures outlined in Art 10(1) – (3) of the LMML "*where a risk assessment has found that the risk is low*" and certain criteria regarding transaction values lower than 150 Euro are fulfilled. This exemption is applied in limited cases in Bulgaria and is subject to control for compliance with the assessment of low risk.

Not all activities that are covered by the FATF definitions for FI and VASP are subject to preventive and supervisory measures in Bulgaria (see R.14, 15, 26 and other preventive measures-related recommendations). In addition, whilst DPMS are exempted from the AML/CFT requirements following the introduction of cash transaction threshold on the basis of risk, the exemption of other activities is not justified.

(b) (N/A)

Criterion 1.7 – Section IV Chapter 2 of the LMML addresses EDD. Art. 35 of the LMML outlines a number of general situations of higher risk where EDD should be applied such as entering into business relationships with entities or natural persons in high risk third countries, transactions that lead to anonymity, new products and delivery mechanisms, new technologies, complex transactions. Art. 49 of the LMML requires FIs and DNFBPs to determine the additional cases in which EDD measures are to be applied.

Pursuant to Art.35 of the LMML, FIs and DNFBPs are required to apply EDD measures in two situations:

i) In specific high-risk situations that are explicitly defined in Art 35 (1) – (7) of the LMML

ii) When a higher risk of ML/TF has been identified according to the procedure established by Chapter Seven of the LMML.

Chapter 7 of the LMML outlines the risk assessment procedures required by FIs/DNFBPs under Art. 98 LMML. Art.98(9) requires that the risk profile of customers shall be determined based on the risk assessments and Art.99 requires that the results of the NRA be taken into account in these risk assessments.

Art. 16-21, 31-33, 34, 41, 43- 46 and Art. 60 (6) of the RILMML outline the procedures and relevant risk factors for assessing the risk, determining the risk profiles of the customers, identifying the areas with higher risk and the application of EDD measures in cases outlined above.

Outside of Art. 35 LMML, Art. 31 – 33 RILMML applies EDD to situations where higher risk has been identified. Art.34 of RILMML applies a specific regime for e-money with additional risk factors to be taken into account. Art. 41 of the RILMML provides requirements on measures when establishing business relationships or effecting an occasional transaction via electronic statement, electronic document or electronic signature, or in any other form without the customers' presence; Art. 43-46 of the RILMML outlines measures applied by NPOs that are similar to EDD measures.

Criterion 1.8 – Section III of the LMML deals with SCDD. Art. 26 permits SCDD in certain general low risk situations and has a requirement for absence of suspicion of ML/TF or involvement of proceeds of criminal activity. However, where the option to apply SCDD remains available, it is not clear how the application of SCDD is based only on situations where lower risks are found based on risk assessments. Pursuant to Art. 98(1) – (8) of the LMML, FIs/DNFBPs are required to conduct their own ML/TF risk assessments and pursuant to Art. 98(9) of the LMML, the risk profile of customers and the type of AML/CFT measures shall be determined based on the risk assessments. Further, Art. 99 of the LMML requires that the results of the NRA should be taken into consideration and reflected in FIs/DNFBPs own ML/TF risk assessments.

Art. 16-21, 31-33, 34, 41, 43- 46 and Art. 60 (6) of the RILMML outline the procedures and relevant risk factors for assessing the risk, determining the risk profiles of the customers, identifying the areas with lower risk and the application of SCDD measures in cases outlined above. Art. 17-21 of the RILMML further regulate the risk factors and the customer risk profile assessment. Art. 23 and 24 of the RILMML provide additional information on how the SCDD is practically introduced, and Art. 34 of the RILMML applies a specific regime for e-money. However, Art. 28 of the LMML allows for SCDD measures to be carried out where the customer is a central or local authority in Bulgaria. It is unclear to the AT whether such circumstances could possibly represent low risk given the identified levels of corruption and potential issues with the effectiveness of some of the competent authorities (see c.10.18) despite the requirement for additional conditions under Art.26 LMML to be met simultaneously.

Criterion 1.9

Art. 114 and 115 of the LMML applies a requirement for a risk-based approach to be adopted when ensuring the control activities for ML/TF are being applied. Art.115 specifically states that

the FID-SANS, BNB, FSC and NaRA shall identify the risk for the purposes of carrying out the inspections under Art. 108 (3) or (6) of the LMML herein when applying the approach referred to in Art. 114 (1) herein.

Art. 108 of the LMML providing for the supervisory powers of SANS, BNB, FSC and NaRA, Art.116-120 of the LMML providing for sanctions for breaches and violations of the provisions cited above in relation to c.1.7 and c.1.8 and for failure to comply with instructions given pursuant to the LMML, e.g. in the case of Art. 103(3) of the LMML.

Criterion 1.10

Section II Chapter 7 of the LMML covers Conduct of Risk Assessment by OEs and Art. 98 of the LMML requires OEs to understand and assess the risks of ML and TF by conducting their own risk assessments, taking into account the relevant risk factors, including those relating to customers, countries or geographic areas, products and services supplied, operations and transactions or delivery channels. Art. 16-20 and 30 of the RILMML covers the risk factors to be taken into account.

(a) Art. 98(7) requires that the risk assessments shall be documented and kept according to the procedure established by Section I of Chapter Three where Art. 67 requires for all documents, data and information collected to be kept for a period of 5 years.

(b) Art. 98(1) states that entities should carry out their risk assessments taking into account the relevant risk factors, including those relating to customers, countries or geographic areas, products and services supplied, operations and transactions or delivery channels. Art. 98 (2) refers to volume of the activity carried out in conducting the risk assessment. Art. 16-21 of the RILMML supplements these provisions.

(c) Art. 98(8) and Art. 99(2) of the LMML requires that risk assessments shall be updated periodically. The time limits, procedure for and additional requirements to risk assessments, as well as the factors which are to be taken into consideration when conducting the risk are outlined in Art. 60 (5) of the RILMML.

(d) Art. 98 (8) of the LMML covers the requirement to have appropriate mechanisms to provide risk assessment information to competent authorities.

Criterion 1.11

(a) Art. 101(1) and (2), items 3-5, 7, 8 and 17 of the LMML requires that FIs and DNFBPS adopt internal rules on control and prevention of money laundering and terrorist financing which shall furthermore be applied effectively with respect to branches and subsidiaries thereof abroad. Art. 60 (6) and 66 of the RILMML contains a requirement for the adoption of policies, controls and procedures and reflecting the ML/TF risk assessments.

Art. 102(3) requires policies, controls and procedures outlined in Art.101 to be adopted by a written instrument of those who manage or represent the FI or DNFBP.

(b) Art. 101(1) and (2), items 3-5 of the LMML and Art. 60 (6) of the RILMML requires internal control, internal audit and independent audit in relation to monitoring the policies, controls and procedures. Art. 101(1) and (2), items 7, 8 and 17 of the LMML and Art. 60 (5) and (6) of the RILMML deals with consideration of ML/TF risk assessments and keeping them up to date.

(c) Art. 49 of the LMML requires FIs and DNFBPs to determine the additional cases in which enhanced customer due diligence measures are to be applied. Art. 16-21, 31-33, 34, 41, 43- 46

and Art. 60 (6) of RILMML outline the procedures and relevant risk factors for assessing the risk, determining the risk profiles of the customers, identifying the areas with higher risk and the application of EDD measures in cases outlined above.

Criterion 1.12

Art. 26 (1), (2) and (6) of the LMML allow for simplified measures only to be applied in low-risk circumstances and where there is no suspicion of money laundering, financing of terrorism or that the proceeds of criminal activity are involved. Art 26 can only be applied where there is no suspicion of money laundering, financing of terrorism or that the proceeds of criminal activity are involved.

Art. 16-21, 31-33, 34, 41, 43- 46 and Art. 60 (6) of the RILMML outline the procedures and relevant risk factors for assessing the risk, determining the risk profiles of the customers, identifying the areas with lower risk and the application of SCDD measures in cases outlined above.

Weighting and Conclusion

Bulgaria has deficiencies in relation to risk assessment, co-ordination and keeping the risk assessment up to date has not yet been demonstrated. In addition, not all activities that are covered by the FATF definitions for FI and VASP are subject to preventive and supervisory measures in Bulgaria and whilst DPMS are exempted from the AML/CFT requirements following the introduction of cash transaction threshold on the basis of risk, the exemption of other activities is not justified. Considering the context and materiality these deficiencies are minor and for these reasons**. R.1 is rated LC**.

Recommendation 2 - National Cooperation and Coordination

Risk assessment

Criterion 2.1 – Art. 96 (1) – (4) of the LMML establishes a standing interdepartmental working group – NRAM WG (see also c.1.2) - to propose measures and action plan for mitigation of the identified in the NRA risks of ML and TF, as well as analyses in the AML/CFT field that require the cooperation between institutions. NRAM WG notably conducted the 2019 NRA and publishes reports based on the results of the 2019 NRA. It draws up proposals on measures to be taken, as well as an action plan for mitigating the risks identified in the NRA (e. g. 2019 NRA Action Plan). There has so far been limited co-ordination and development of ML/TF policies concerning the risk that VASPs present in Bulgaria. Whilst the area was generally covered in the NRA this was only generally covered and without a more detailed risk assessment of the sector the implementation of risk-based ML/TF policies remains challenging.

Criterion 2.2 – The standing interdepartmental working group (permanent interagency working group) – NRAM WG - established under Art.96 of the LMML acts as the national coordination mechanism in the area of AML/CFT policy.

Criterion 2.3 – The standing interdepartmental working group (permanent interagency working group) established under Art. 96 of the LMML contains all public stakeholders which enables policy makers and competent authorities to co-operate and where appropriate, co-ordinate and exchange information domestically, with each other concerning the development and implementation of policies and activities.

Coordination of operational activities is done both at the level of the working group under Art. 96 of the LMML and bilaterally/multilaterally between the authorities through joint instructions and

ad-hoc or permanent working groups depending on the area of competence and cooperation. There remain significant challenges in operational co-operation between the law enforcement agencies and FIU.

According to Art. 96(5) of the LMML, the members of the working group shall be obliged to provide the working group with the information and data, including the statistics referred to in Art. 71 of the LMML, that are necessary for the working group to perform its tasks. These include not only to conduct and update the national assessment of the risk of money laundering and terrorist financing in the Republic of Bulgaria (Art. 96(1), item 1 of the LMML), but also activities related to development and implementation of AML/CFT policies. Note also, Art. 59 of the RILMML regarding reports to the Council of Ministers.

Criterion 2.4 – The Bulgarian authorities established a working group in 2019, which is responsible to draft law on international restrictive measures. However, a final draft of the law is not yet available. There is no co-operation mechanism beyond the work on the draft law.

With an act of the Council of Ministers No 50/01.03.2012 the SANS is appointed to carry out the counterproliferation coordination between the competent authorities. Each authority has nominated an officer to act as point of contact (PoC) for rapid exchange of information or advice on reaching appropriate structure in the relevant organization. The list of PoC is periodically updated. The PoC have regular meetings to discuss specific topics or discuss general threat assessment of the environment. If operational cooperation is needed this is done on an ad hoc basis via the PoC of each competent authority. Political level co-operation also occurs at Council of Ministers level where required.

Criterion 2.5 – NRAM WG established under Art.96 of the LMML contains authorities with competences in data protection where this area interacts with the AML/CFT legislation.

Representatives of the Commission for Personal Data Protection (CPDP) participated in meetings of the ad-hoc working group (mentioned in c.2.2) in relation to the transposition of 4AMLD and 5AMLD where the elements of personal data protection were considered.

The relevant provisions of LMML and LMFT that take into consideration the requirements of the General Data Protection Regulation are: Art. 83 and paragraph (para.) 4 of the supplementary provisions of LMML and para. 1c of the supplementary provisions of the LMFT.

Weighting and Conclusion

Bulgaria has deficiencies in relation to effective co-ordination mechanisms for developing and implementing national AML/CFT strategies and particularly ensuring that those strategies are adequately informed by risks. Given the risk profile and number of authorities concerned in risk assessment and national policy development in Bulgaria, significant weighting is given to c.2.1. There have not yet been any specific national policies developed based on risk understanding, apart from the actions contained in the 2019 NRA Action Plan which was only formally adopted during the onsite (c.2.1., c.2.3 and c.2.4). For these reasons, **R.2 is rated PC.**

Recommendation 3 - Money laundering offence

Bulgaria was rated LC for the previous R.1 in the 2013 MER whereas Recommendation 2 (which also makes part of the present Recommendation 3) was not assessed. In addition to concerns regarding effectiveness, two technical deficiencies contributed to this rating, namely that the definition of "property" did not include indirect proceeds and that not all the designated

categories of predicate offences were covered by the CC. As far as the first deficiency is concerned, the situation has remained largely the same.

Criterion 3.1 - The 2013 MER provided for a detailed analysis to demonstrate that the Bulgarian CC covered the scope of ML offence in almost all the material elements required by the international standard regardless of some minor differences in the wording of Art. 253 CC (e.g. as regards the coverage of "*conversion*" and "*transfer*") which was accepted by the present AT as well. Indeed, in terms of the mental element, the Bulgarian ML offence goes beyond the standards (e.g. by not requiring any purpose for conversion and transfer).

There appeared to remain, however, a technical deficiency that whereas "*concealment*" is clearly covered by the ML offence, there is no mentioning of "*disguise*". While Bulgarian authorities argued, both in the present and in the previous rounds of evaluation, that the Bulgarian term used in the ML offence clearly covers both activities. Concealment and disguise are, however, two similar, yet clearly distinguishable terms in most relevant international instruments such as the Vienna and Palermo Conventions, which are translated accordingly, by use of two different Bulgarian terms, in the official Bulgarian version of the said treaties. Leaving one of these out from Art. 253 of the CC was thus considered a clear shortcoming also in the previous MER, even if it was admittedly remedied, to some extent, by broad interpretation of the law.

The Bulgarian authorities, however, succeeded to demonstrate by a recent Supreme Court decision (No 121 dated 08.10.2020 on criminal case No 422/2020) that, in the context of the ML offence, the judicial practice unequivocally considers the term "concealment" broad enough to entirely cover all activities referred to in the said international treaties as "concealment and disguise". This guiding decision, which is in line with a previous Supreme Court decision of 2005 (see footnote 17 page 44 of the 2013 MER) gives a definition for the term "concealment" as used in the ML offence. This term, which the court clearly considers to be equal to the concept of "*concealment and disguise*" as used in the UN Convention against Corruption and the CoE Warsaw Convention thus "*should be understood as any act which, by its nature, is intended [to hamper] or results in hampering the authorities or those having rights over the relevant objects, in the knowledge of their nature, origin, location, movement or actual rights related to them*".

In light of this, the AT is ready to accept that even if "conceal" (*prikriva)* and "hide" *(ukriva)* are two different verbs in the Bulgarian language, the term "conceal", as used in the ML offence, not only has a broad and inclusive meaning potentially covering both "concealment" and "disguise" but this interpretation has been manifested in multiple guiding decisions of the Supreme Court as well. As a result, this apparent and arguable technical deficiency has adequately been remedied by case law.

Criterion 3.2 – Bulgaria follows an all-crime approach thus all the criminal offences penalised in the Special Part of the CC constitute predicate offence for ML. Those designated offences which had not been criminalised by domestic legislation at the time of the previous assessment (insider trading, market manipulation and piracy committed on ships) have since been included in the Criminal Code and are now predicates for ML without exception (see new Art. 260a - 260c and Art. 314b as amended).

Furthermore, the ML offence refers to proceeds of "crime or another act that is dangerous for the public" where the latter term may equally refer to an administrative offense, an audit act of a control authority or a civil tort, as well as an act that formally covers the elements of a crime but for some reason (e.g. the perpetrator has died or cannot be held criminally liable) it cannot be prosecuted. As a result, the ML offence can theoretically be applied to proceeds of non-crimes too,

which clearly goes beyond the FATF standards, although there have been no such cases in practice.

Criterion 3.3 *(N/A)* – Bulgaria does not apply a threshold approach or a combined approach that includes a threshold approach. This criterion is not applicable.

Criterion 3.4 – While the term "*property*" is frequently used in the CC (including the ML offence in Art. 253) the AT could find no legal provision to define the scope of this term within the context of the CC.

The situation is largely the same as it was at the time of the 4th round assessment, when authorities referred to different legal norms, from the Strasbourg and Warsaw Conventions to the 2006 Law on Recognition, Enforcement and Issuance of Writs for Securing of Property or Evidence (abbreviated as REIWSPE) as the source of the definition of "property". A recommendation was made that a clear definition of "property" (including the referral to both direct and indirect proceeds) should be adopted in the legislation, or, at least, a clear indication should be provided as to what legal document is to be taken into consideration when defining "property" for ML purposes.

This recommendation has not since been met and the present AT is not convinced of the direct applicability of any specific legal norm to define the term "property" for the purposes of the CC. The definitions raised by the Bulgarian authorities, namely, the one in REIWSPE (Additional provision § 1. para [3]) and another one in the LCCIAF (Additional provisions §1 para [4]) are slightly different and clearly restricted for the purposes of the respective Acts. There are other competing definitions for "property" such as the one in the Law on the Measures Against Money Laundering (Supplementary provision §.1 [22]) but also the one in the 1951 Property Law (Art. 110 - 111) which all show a certain level of discrepancy and there is no clear legal provision to render any of these generally applicable in the wider context of the CC.

That said, however, most of these definitions are largely in line with the respective Glossary definition and the AT accepts that both these and those in the Strasbourg and Warsaw Conventions might theoretically be applied for the ML offence by virtue of Art. 37 (1) of the Decree No 883 on the application of the Law on the normative acts ("*words or expressions with established legal meaning shall be used in the same sense in all normative acts*"). There is no rule in Bulgarian law to exclude the applicability of the ML offence to property consisting of virtual assets (VAs).

While the ML offence remains silent on whether it extends to property that indirectly represents the proceeds of crime, the Bulgarian authorities demonstrated that in the practice of ML criminal cases, it is accepted that any property arising directly or indirectly from the original crime, either derived from or received for its commission, may equally be subject of ML. This interpretation was corroborated by jurisprudence of the Supreme Court of Cassation (see Judgement No. 34 of 10.03.2009 in case no. No. 577/2008 and subsequent SCC case law).

Criterion 3.5 – As it was already pointed out in the 2013 MER, the prior conviction for the predicate offence is not required by Bulgarian law as a precondition to prove that the property is proceeds of crime, as it is implied by the wording of Art. 253(1) CC. This legal principle had already been confirmed by a Supreme Court decision before the 4th MONEYVAL assessment and has since been consequently applied in the jurisdiction of the Supreme Court and generally in the practice of the criminal courts of Bulgaria.

Criterion 3.6 – Art. 253 (7) CC expressly extends the scope of the entire ML offence to proceeds from predicate offences that fall outside the criminal jurisdiction of Bulgaria.

Criterion 3.7 – Laundering of own proceeds is entirely, although implicitly, covered by the ML offence under Art. 253 CC which makes no exception as to the perpetrator of the predicate crime. This conclusion had already been confirmed by case law at the time of the previous assessment.

Criterion 3.8 – Art. 104 CPC expressly provides that evidence in the criminal proceedings may be factual data related to the circumstances in the case, such that contribute to their elucidation and are ascertained by the procedure provided for by the said Code. As it was pointed out by the authorities, the long-established practice of law enforcement and judicial authorities to prove the subjective side of any crime (knowledge, intent, purpose etc.) is indeed based on drawing inferences from all objective circumstances. The AT thus shares the conclusion already drawn in the 2013 MER (there in relation to SR.II) that the intentional element of the TF offence can be inferred from objective factual circumstances.

Criterion 3.9 – The criminal sanctions available for the basic and aggravated forms of the ML offence are undoubtedly dissuasive and, in most cases, also proportionate. The basic ML in Art. 253 (1) CC is punishable by imprisonment of 1 to 6 years and a fine of 3000 to 5000 BGN (€1 534 - €2 557) while the more serious forms in paragraphs (3) to (5) carry proportionately higher sentences up to imprisonment from 5 to 15 years. The severity of these sanctions is in line with those available for other serious economic offences in the CC.

There is, however, one issue disrupting the proportionality of the sanctioning regime. The rate by which the range of additional fines increase for the more and more aggravated forms of ML unexplainably differs from the rate used for imprisonment sanctions. While imprisonment sanctions for serious forms of ML are 1 to 8 years, 3 to 12 years and 5 to 15 years, the respective fines that can be applied together with these imprisonment terms are 5000 to 20 000 BGN (€2 557 to €10 229), 20 000 to 200 000 BGN (€10 229 to €102 293 and), surprisingly, 10,000 to 30,000 BGN (€10 229 to €15 344). Even if the latter, most severe form of ML is threatened with a third sort of sanctions consisting of deprivation of the right, first, to hold a certain state or public office and second, to exercise a certain vocation or activity (Art. 37.§ [1] 6-7) this cannot counterbalance the disproportionately low amount of fines applicable for such cases of ML.

Criterion 3.10 – The Bulgarian legislation does not envisage criminal liability for legal persons. The principle for the personal character of the criminal liability is considered a fundamental legal principle existing since the adoption of the Bulgarian Criminal Code in 1968. While this is undoubtedly a basic principle of the criminal law, it still does not seem to amount to a "*fundamental principle of domestic law*" as defined in the Glossary to the FATF Methodology (contained or expressed in the national Constitution, or similar document etc.)

As at the time of the previous round of MONEYVAL assessment, the liability of legal persons is regulated under the Administrative Violations and Sanctions Act of 1969 (Art. 83a to 83g) according to which a legal person, which has enriched itself or would enrich itself from a range of criminal offences (including ML and TF) shall be punishable by an administrative liability. This approach was found insufficient in the 2013 MER (when assessed under the then Special Recommendation II) and a recommendation was made to introduce corporate criminal liability. As a result, the Administrative Violations and Sanctions Act was amended in 2015 introducing a "*quasi criminal*" corporate liability with the proceedings being conducted by a criminal court. That is, while the proceedings remained administrative, the amended law now provides for the subsidiary application of the Criminal Procedure Code thus enabling the use of investigate tools envisaged in the CPC as well as the mutual legal assistance.

The administrative liability thus depends on whether the legal person has enriched or would have enriched itself from a crime committed, attempted, abetted, or assisted by a natural person having a leading or decisive position in the same legal entity (such as a representative, an elected official in a control or supervisory body or a responsible employee). The criminal offences for which this scheme applies encompass ML and TF with a wide range of proceeds generating offences and, in addition, any other crimes if committed upon order of an organised criminal group. The administrative liability of the legal entity applies regardless of the materialization of the criminal responsibility of the natural person.

In lack of demonstrable enrichment from a criminal offence, however, the legal person cannot be held liable (which may easily occur in case of legal entities used to channel funds for the purpose of ML or TF). Furthermore, the only sanction applicable is a financial penalty not less than the amount of the actual enrichment (benefit) but maximum 1000000 BGN (€511 465) with no possibility for other sanctions such as the suspension or termination of the legal person. The sanctions thus cannot be deemed proportionate or dissuasive.

Criterion 3.11 – The requirements of this criterion were found to be satisfied in the 2013 MER. The respective CC articles have since remained unchanged: Art. 253a (1) of the CC on preparation towards ML or association to commit ML, read together with the general rules on preparation in Art. 17 of the CC (covers association with, or conspiracy to commit ML), Art. 18 of the CC on attempt (applicable to all intentional crimes), Art. 20 of the CC on perpetrators, abettors, and accessories (covers all forms of participation, aiding, abetting, facilitating, and counselling, applicable to all intentional crimes) plus a specific rule in Art. 253a (2) of the CC on abetting to ML. These provisions undoubtedly meet all requirements under c.3.11 (while the anomaly in sanctioning the abetting to ML is to be discussed under c.3.9 above).

Weighting and Conclusion

The criminal sanctions available for natural persons are dissuasive but the system of additional fines is not sufficiently proportionate. There is no corporate criminal liability and the administrative liability of legal persons for criminal offences is limited. **R.3 is rated LC**.

Recommendation 4 - Confiscation and provisional measures

Bulgaria was rated PC on former R.3 in the 2013 MER. Apart from issues arising about the effectiveness of the general confiscation regime, the factors underlying the rating were mostly technical, such as the limited scope of third party confiscation (in case of instrumentalities and the object of crime), the rights of bona fide third parties not being protected in all circumstances, the lack of definition of property subject to security measures and the deficiencies in ML/TF criminalization having an impact on the applicability of the seizure and confiscation measures.

Since the adoption of the 2013 MER the criminal confiscation and provisional measures have not gone through any substantial changes and therefore most of the deficiencies appear to prevail. This regime continues to be supplemented by a parallel civil confiscation mechanism currently provided by the LCCIAF of 2018 - quite similarly to the previous regime established by predecessor legislation already being in force at the time of the previous Moneyval evaluation.

Criterion 4.1 – The confiscation regime set out in the CC is based on two main legal instruments: the confiscation of existing property, which is a criminal punishment (Art. 44-46) and the confiscation measure in Art. 53 CC. While both are translated as "confiscation" in English, these are two separate measures in Bulgarian terminology (*konfiskatsiya* vs. *otnemane*). The confiscation in Art. 44-46 CC (hereinafter: "confiscation of property") is a criminal sanction by

which the assets of the convicted person (either the entire property or parts thereof) are compulsorily appropriated in favour of the state without compensation. While a robust measure, this sort of punishment cannot be tested against the FATF standards and thus will not be discussed more in details. In contrast, the measure in Art. 53 CC (hereinafter "confiscation") does correspond to the FATF concept and definition of confiscation, extending to instrumentalities, intended instrumentalities and proceeds alike. Art. 53 CC is a general provision applicable to all crimes set in the Criminal Code, which is supplemented by specific confiscation measures attached to the ML and TF offences in Art. 253 (6) and Art. 108a (8) respectively. All these provisions extend to "*objects*" (in the 2013 MER translated as "*things*") which term was found already in the 2013 MER to cover both movable and immovable assets. There is no rule in Bulgarian law to exclude the applicability of the confiscation or provisional measures to virtual assets.

(a) Confiscation of the object or body of an intentional criminal offence (*corpus delicti)* is generally provided for by Art. 53 (1)(b) CC but only if it belongs to the perpetrator (except if the possession of the item in question is forbidden, where there is no such limitation) and without the possibility for a value confiscation. The confiscation measures under Art. 53 (1) CC apply irrespective of criminal liability and can thus be imposed also in lack of conviction (e.g. in case of the death of the perpetrator). For the purposes of the ML offence, however, this general rule is significantly extended by a *lex specialis* provision in Art. 253 (6) stipulating that not only the object or *corpus* of the ML offence (i.e. the laundered property) is to be confiscated but also the property into which it has been transformed, as well as the equivalent value if the original or the transformed property is absent or alienated. As opposed to the general rule, the specific provision in Art. 253 (6) is not restricted to property that belongs to the perpetrator and, as it was demonstrated by case law, it does extend to third party confiscation.

(b) Proceeds of crime are to be confiscated pursuant to Art. 53 (2)(b) which extend to direct or indirect benefits gained from crime unless such benefit is not subject to return or restoration. If the property constituting such benefit is absent or alienated, its equivalent shall be confiscated. A detailed explanatory provision in Art. 53 (3) makes it clear that "indirect proceeds" are covered fully in line with Criterion 4.1 (b).

Confiscation of instrumentalities and intended instrumentalities of an intentional crime is generally provided under Art. 53 (1) (a) CC together with a possibility for value confiscation in cases mentioned above. On the other hand, however, (intended) instrumentalities can only be confiscated if they belong to the perpetrator and therefore this measure does not apply to third persons. The confiscation of (intended) instrumentalities can also be applied in lack of a conviction (see above).

The mechanism for confiscating proceeds of crime is completed by the LCCIAF (and the quite similar preceding legislation from 2012) introducing a civil confiscation regime by which assets, for the acquisition of which a legitimate source has not been identified, shall be treated as unlawfully acquired and thus subject to civil forfeiture, without prejudice to steps and measures taken under other laws, including the commencement of a criminal proceeding.

The Commission shall institute an unlawfully acquired assets forfeiture proceeding where a reasonable assumption can be made, on the basis of an examination carried out by the competent territorial director of the CACIAF, that particular assets have been acquired unlawfully, including by a person accused or suspected of any of the proceeds-generating criminal offences listed in Art. 108 of the said law (including ML and TF). Whenever a formal accusation for any of these

crimes takes place, or even without an accusation if it was prevented by specific reasons (amnesty, death or abscondment of the perpetrator, etc.) the CACIAF examination will be triggered by a notification from the prosecutor supervising the respective pre-trial proceeding or case file. As a result of a thorough examination, the CACIAF can bring an action for forfeiture of unlawfully acquired assets before the competent district court. Unlawfully acquired assets are to be forfeited not only from the accused but also from third parties.

(c) Art. 108a (8) of the CC provides that the object of the TF offence or, if it is absent or has been alienated, its equivalent value shall be confiscated. This is again a *lex specialis* to the general rule in Art. 53 (1)(b) of the CC extending its scope beyond the property that belongs to the perpetrator and providing for value confiscation. This provision adequately covers property "used in" a TF offence while proceeds of the same are covered by Art. 53 (2) (b) of the CC as discussed above.

As regards property "intended or allocated for use" in relation to TF, these are covered beyond doubt if the commission of the TF offence has at least been attempted (which is a punishable act by itself). If only preparation for TF can be proven (e.g., the mere allocation of one's own funds for terrorist purposes) it can only be punishable, by virtue of Art. 110 of the CC, if it constitutes a preparatory act for a terrorist offence in Art. 108b (1) of the CC that is, if the funds are specifically intended/allocated for use to carry out a terrorist act, but not to be used by a terrorist organisation or individual terrorist for any purpose, for which case there is no clear provision to be found.

(d) As noted above, value confiscation generally applies to proceeds of crime and to the subject or *corpus* of the ML offence. Equivalent value of instrumentalities or intended instrumentalities can only be confiscated if they belong to the perpetrator. Value confiscation can take place if the original property item can no longer be found, or it has been transferred to someone else– which in practice extends to cases where the original property item is unidentifiable and/or merged with the lawful property of the defendant or another person.

Value confiscation also applies in the asset forfeiture proceedings initiated by the CACIAF (see Art. 142 of the respective Law).

Criterion 4.2

(a) For the purposes of criminal procedure, one can find no explicit norms (either in the CPC or another law) for regulating the identification and tracing of property to be confiscated. As noted above, Art. 109 CPC requires that material evidence including (intended) instrumentalities and the subject of the crime be collected, while Art. 102 stipulates that the "*family or financial status*" of the defendant is one of the subjects that need to be proven in the criminal proceedings and thus indirectly authorizes the pre-trial bodies to collect evidence also in this context.

Acting upon this authorization, though, the pre-trial bodies have access to a variety of sources to identify and trace property, mainly based on bilateral agreements between the Prosecutor's Office of the Republic of Bulgaria and the respective governmental bodies (CACIAF, State Financial Inspection Agency, National Revenue Agency, etc.) or by access to databases (BNB Register, real estate register, commercial register, MoI register of vehicles etc.) Data and documents held by these entities can be requested by virtue of Art. 159 (1) of the CPC while information covered by bank secrecy can be obtained by an order issued by the competent district court pursuant to Art. 62 (6) of the CIA.

Completing the criminal confiscation mechanism above, however, the LCCIAF provides for a thorough and detailed mechanism for identifying unlawfully acquired assets. Once the

examination referred to under C.4.2 (b) above has been initiated (upon notification of the competent prosecutor) the respective territorial directorate and its inspectors have maximum 1 ½ year to examine and identify unlawful assets acquired in the preceding 10 years (Art. 112 of the CPC). Specific powers available to these authorities are stipulated in Chapter 11 of the said Law, by which they can gather information on all relevant aspects of the assets and the property status of the respective natural or legal person, requesting data and information from any relevant sources (including information covered by bank or trade secrecy the lifting of which can be requested from the court).

(b) Art. 109 of the CPC prescribes that objects intended or used for the perpetration of the crime, objects upon which there are traces of the crime or which were subject of the crime, as well as all other objects which may serve to elucidate the circumstances in the case are to be collected as material evidence. For this purpose, the provisional measures of search and seizure are available under Articles 159 to 165 of the CPC which, however, cannot generally be applied for securing property subject to confiscation. In this regime, a physical object, a document, or digital data can only be seized if it constitutes evidence in the criminal proceedings, which term thus includes (intended) instrumentalities and the object (*corpus*) of the criminal offence, but not the proceeds thereof. Search and seizure must be authorised by the competent court of first instance, except in cases of urgency, where the pre-trial (investigative/prosecutorial) authorities may proceed without judicial authorisation, but it must be obtained within a 24-hours deadline. Search and seizure can be made *ex-parte* or without prior notice.

The CPC provides for another regime for securing property subject to confiscation which operates on measures stipulated under the Code of Civil Procedure (CCP). Art. 72 of the CPC provides the competent court of first instance the possibility to apply measures, at the request of the prosecutor, to secure the fine, the confiscation of property (Art. 44 CC) and the confiscation (Art. 53 CC as well as additional confiscation provisions, such as the one in Art. 253 [6] of the CC) pursuant to the procedure set forth in the CCP. The latter refers to measures and procedures in Part Four of the CCP (Precautionary proceedings) including proceedings for granting injunction (Chapter 34) and the applicable precautionary measures (Chapter 35). Precautionary or security measures in Chapter 35 include placing interdict on a real estate, imposing garnishment (distraint) on movable objects and receivables of the debtor, as well as any other appropriate measures determined by the court (Art. 397). Neither the CPC nor the CCP contain explicit definition of property subject to these measures (which thus only extend to real estate, movable objects, and "receivables").

An injunction securing the action will only be granted if, without such an injunction, it would be impossible or difficult for the plaintiff (i.e. the prosecutor) to realize the rights under the judgment (Art. 391). Furthermore, pursuant to the binding case law[107]it is necessary in all cases for the owner of the property, in respect of which the prosecutor has made a request for imposition of precautionary measures, to be brought as an accused for a crime for which a fine and/or confiscation of property (i.e. the punishment in Art. 44 of the CC) is envisaged. This appears to be an unreasonably narrow (or even *contra legem*) interpretation of Art. 72 of the CPC, plainly excluding crimes not punishable by a fine or confiscation of property such as the TF offence in Art. 108a (2) of the CC, which may easily have a negative impact on the application of the underlying provisions.

[107]Interpretative decision No. 2 of 11.10.2012 of the Supreme Court of Cassation

Having said that, it is therefore impossible to apply these measures before the formal accusation of the owner of the respective property, and also to apply such measures to property held or owned by third parties. On the other hand, these measures can be executed *ex-parte* and without prior notice: upon request of the applicant (i.e. the prosecutor) the distraint is imposed immediately and a notification instead of summon for voluntary execution will be served on the defendant, while the imposition of an interdict is done by registering the security order of the court anyway, of which the defendant will only be notified afterwards (Art. 400 CCP).

The LCCIAF provides for a similar mechanism for securing property in asset forfeiture proceedings initiated by the CACIAF. The Commission adopts a decision on submission to the competent district court of a motion for an injunction securing a future action for forfeiture of assets on the basis of a report made by the director of the territorial directorate concerned, where sufficient data have been collected, raising a reasonable presumption that the said assets have been acquired unlawfully (Art. 116). The available precautionary measures are exactly the same as mentioned above (see Art. 397 CCP) and the procedure provided under the LCCIAF is in most aspects very similar to the one stipulated in Chapters 34 and 35 of the CCP (including the preconditions for and the ex-parte applicability of the measures.) As opposed to the CCP, this Law provides for an appropriate definition of "assets" (see C.3.4 above) with detailed rules for various sorts of property, and also defines that the precautionary measures shall extend to the interest, as well as to other civil fruits derived from the respective assets.

(c) The possibility to void contracts is provided for, in general terms, under Art. 135 of the Law on Obligations and Contracts according to which the creditor (i.e. the State in case of confiscation) may require that any acts of the debtor that damage the creditor be declared void, if the debtor was aware of the damage when performing those acts. Voidance shall not affect the rights acquired in good faith by third parties prior to the registration of the claim for voidance.

In addition to that, and specifically in asset forfeiture proceedings initiated by the CACIAF, Art. 143 of the LCCIAF prescribes that any transaction effected in unlawfully acquired assets shall be ineffective in respect of the State and the consideration given under any such transactions shall be forfeitable provided that the said transactions are gratuitous transactions with natural or legal persons, or onerous transactions with third parties, if the said parties knew or could have presumed that the assets had been acquired unlawfully or if the said parties acquired the assets for the purpose of concealing the unlawful source thereof or the actual rights related thereto.

(d) As far as the powers of the pre-trial authorities in the criminal proceedings are concerned, there is no obstacle to take all appropriate investigative measures within the context of C.4.2.

Criterion 4.3 - Protection of third-party rights is to be examined where third party confiscation applies (and thus not in case of [intended] instrumentalities, which can only be confiscated if held or owned by the perpetrator).

As far as confiscation of proceeds of crime is concerned, the possibility for value confiscation under Art. 53 (2)(b) CC (to substitute assets that have already been expropriated) is generally interpreted to protect the rights of the third party, who has purchased the original property item in good faith, and the same goes for the confiscation of laundered property under Art. 253 (6) CC. Bona fide acquisition is interpreted in accordance with the Law on ownership, which provides that good faith is always presumed until proven otherwise.

Since the provisional measures' regime operates through a mechanism applying civil measures provided by the CCP, the procedural provisions for protecting third party rights are necessarily

those provided in this Code and not in the CPC. In this context, Art. 396 CCP provides that the ruling of the court on an injunction can be appealed by the respondent (including third parties). In addition, the third party can use various avenues provided by the CPC to protect his rights, including bringing an action to restore a right that has been impaired (Art. 124) an action for remedy against disturbed possession and holding (Art. 356.) or seeking remedy against the enforcement of a precautionary measure that has affected their rights (Art. 440).

This equally refers to the asset forfeiture proceedings initiated by the CACIAF which also operate through or similarly to the CCP provisions (e.g. the right to appeal under Art. 396 CCP is identically provided under Art. 117 of the LCCIAF). Article 154 of the latter Act provides that an action for the forfeiture of illegally acquired assets is brought not only against the person subject to inspection but also those who have acquired the property, all these being independent parties to the proceedings with full procedural rights.

Art. 143 of the same Act explicitly defines mala fide transactions (rendering them ineffective) thus protecting property rights derived from onerous transactions with third parties acting in good faith. If property constituting proceeds or laundered assets have been acquired and held or owned by a third party and this property is confiscated by the court, the third party has its independent right to appeal and also to seek compensation for damages under the general law against persons from whom they acquired the property.

Criterion 4.4 – Management of seized and confiscated assets is carried out by the CACIAF through a single and detailed mechanism set out in Chapter 13 of the LCCIAF. While this mechanism primarily extends to assets subject to provisional (precautionary) measures and forfeiture under the civil confiscation regime established by the said Act, it also applies to property secured for the purposes of confiscation under the Criminal Procedure Code by virtue of Art. 72a CPC. Chapter 13, however, does not appear to provide for active management of property or property items beyond safekeeping measures until they are disposed.

Storage and safekeeping (but no active management) of property items seized as instrumentalities or the object of crime is also provided as these constitute physical evidence. In this case, safekeeping is carried out by the competent PPOs or their respective investigative bodies according to the Rules for the Administration of the Prosecutor's Office of the Republic of Bulgaria (PAPRB of 2013 as amended).

There is no mechanism available for managing and disposing of property that has been confiscated under the Criminal Code.

Weighting and Conclusion

Instrumentalities and intended instrumentalities of a criminal offence can only be confiscated from the perpetrator and not from third persons. There is no clear provision for all aspects of the confiscation of property "intended or allocated for use" in relation to TF. Unless the respective object (property item) constitutes material evidence in the criminal proceedings (and thus can be subject of seizure pursuant to the CPC) the provisional measures cannot be applied before a formal accusation takes place and neither can they be applied to third parties (this also refers to the asset forfeiture proceedings by the CACIAF). For the purposes of applying provisional measures in the criminal procedure, there is no explicit definition of property subject to these measures. There is no mechanism available for the active management of seized and confiscated assets beyond storage and safekeeping measures, and for managing and disposing of property that has been confiscated under the CC. **R.4 is rated PC.**

Recommendation 5 - Terrorist financing offence

In 2013 MER, Bulgaria was rated PC on old SR.II. The factors underlying this rating were: (i) not all acts defined in the treaties listed in the Annex to the TF Convention were criminalised; (ii) the purposive element for the terrorist offence was extended to the treaty offences and thus limited the scope of the TF offence; (iii) the TF offence did not cover threatening/forcing a competent authority, a member of the public or a foreign state or international organisation to perform or omit from doing any act; (iv) the term "fund" was not defined under the criminal legislation and there was no explicit coverage of funds, which are to be used in full or in part; (v) the act of providing or collecting funds for any purpose was not criminalized and (vi) criminal liability was not applied with regard to legal persons.

Following the adoption of its 4th round report in 2013, Bulgaria was placed in regular follow-up and then under the Compliance Enhancing Procedures (CEPs) procedures, during which the respective CC articles were amended multiple times. 1st Compliance Report of July 2018 found that Bulgaria had addressed most recommended actions on SR.II from the 4th round MER (see discussed below) which brought the level of compliance with SR.II to LC. The CEPs procedures were lifted in July 2018. Since then, no significant changes have been brought to the relevant legislation.

Criterion 5.1 – As noted above, Bulgaria has significantly amended its TF offence and other related CC provisions during the regular follow-up and compliance enhanced procedures (CEPs) procedures, as a result of which both key criminal offences, that is the TF offence in Art. 108a (2) CC and the terrorism offence in Art. 108a (1) of the CC have been brought more in line with the TF Convention.

At the time of the previous MONEYVAL assessment, the majority of the conducts prescribed in the 9 conventions and protocols listed in the Annex to the TF Convention were not criminalised in Bulgaria and thus could not be subject of terrorist financing either. This deficiency affected 6 out of the 9 "*treaty offences*" at that time. Most of these 6 conducts have since been criminalised by amendments to the Bulgarian CC as it is demonstrated in detail in the 1st Compliance Report of July 2018 where it is concluded that 4 of the 6 conducts are now fully covered. The remaining two are, first, the offence provided by the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents which was found to be "*mostly covered*" and the offence in the International Convention for the Suppression of Terrorist Bombings which is "*not fully covered*". As to the former, the AT agrees with the Compliance Report in that the broad interpretation of the existing provisions gives room to conclude that all aspects of this "*treaty offence*" are at least implicitly covered by the Bulgarian law. As to the latter, however, it is beyond doubt that not all aspects of the respective conduct are criminalised, so the coverage remains incomplete.

All the CC articles by which the aforementioned "*treaty offences*" are criminalised are now listed under Art. 108a (1) of the CC and are therefore included in the concept of the terrorism offence, which means that support provided in relation to any of such conducts will necessarily be qualified as terrorist financing.

The terrorism offence itself is made up of a broad list of various criminal offences including but not limited to the articles covering the nine "*treaty offences*". The coverage of the "*general*" terrorism offence in Art. 2 (1)(b) of the TF convention is thus achieved through reference to a number of other criminal offences (such as murder in Art. 115 of the CC or bodily injury in Art. 128) of the CC if committed with a specific purpose.

Deficiencies of this purposive element had already been criticised in the 2013 MER such as the purpose required for committing the terrorism offence, which was more specific than what is prescribed by the TF Convention (making reference to the respective entities being threatened or forced to perform or omit whatsoever as "*part of their duties*" which is an addition to the language of the Convention). This deficiency has since been remedied by deleting the additional purposive element from the terrorism offence as recommended in the 2013 MER.

Second, the same purpose was required for all offences constituting the terrorism offence under Art. 108a (1) which clearly included all offences serving to criminalise the acts listed in the nine Conventions and Protocols to the TF Convention. Pursuant to Art. 2 (1)(a) of the TF Convention, these "treaty offences" should not contain a reference to such intentional element and thus requiring a purpose for those acts will automatically restrict the scope of the terrorism offence – and that of the TF offence also. This shortcoming has not yet been remedied.

Criterion 5.2 – The TF offence in Art. 108a (2) now prohibits the provision or collection of financial or other means, regardless of the mode of operation (i.e. by any means) directly or indirectly, with the knowledge or assumption that they will be used, entirely or partially:

(a) for committing any of the terrorist acts listed in Art. 108a para (1) i.e. the basic terrorism offence roughly covering both Art. 2 (1)(a) and (b) of the TF convention (see above under C. 5.1) as well as para (3) and (4) on terrorism-related recruitment and training, and para (6) and (7) on travelling for terrorist purposes

(b) by a single terrorist, defined by having committed any of the aforementioned terrorist acts

(c) or by a terrorist group or organisation, defined by its goal of committing a crime under para (1) or (3).

Financing of a terrorist group or an individual terrorist should be established even in the absence of a link to a specific terrorist act or acts. Terrorist groups or organisations, as mentioned above, are defined by their goal of committing a future terrorist act which thus cannot be considered a "specific" terrorist offence. The same cannot be said, however, about the individual terrorist who is defined by having committed a concrete terrorist act and thus his financing will necessarily be linked to a specific terrorist offence.

A certain part of the mental element (intent as opposed to knowledge) is not expressly covered, but this appears to be adequately counterbalanced by lowering the knowledge standard to the level of assumption, as a result of which no criminal conduct seems to have been left uncovered.

On the other hand, the TF offence does not extend to "other assets" that is, beyond the concept of "funds" as required by the current FATF Methodology (see under c.5.3).

Criterion 5.2bis – Art. 108a (6) CC penalizes Bulgarian citizens who leave Bulgaria across its border for the purpose of getting involved in a crime under paragraphs (1) to (4) of the same article, including any crime against another country. The offences in the said paragraphs are the terrorist act, the financing of terrorism, the recruitment and training of others for the purpose of committing a terrorist act, and the receiving of training for the same purpose. The TF offence in Art. 108a (2) clearly extends to financing the activity criminalised in paragraph (6) the broad wording of which, together with the range of the offences that make up the purposive element, leave no doubt that, as far as the travel of Bulgarian nationals to abroad is concerned, all aspects of Criterion 5.2bis are covered.

Art. 108a (7) CC provides that foreign national shall be punished for entering Bulgaria across its border for the purpose of getting involved in any of the crimes under paragraphs (1) to (4) or for illegally residing in Bulgaria with the same purpose. The TF offence extends to the financing of these activities also.

There appears however no provision to criminalize foreign nationals legally residing in Bulgaria who decide to travel abroad for the purposes mentioned above (because para [6] dealing with travelling abroad only covers Bulgarian nationals). The same goes for Bulgarian citizens living abroad, who enter Bulgaria to recruit or to train others for the purpose of committing a terrorist act or to receive training for the same purpose (which acts, if consummated, would fall under Art. 108a [3] and [4] of the CC – but preparation for the same acts is not a *sui generis* crime under Art. 110[1] CC). Consequently, the TF offence does not extend to the financing of such activities and thus the coverage of Criterion 5.2bis is incomplete.

Criterion 5.3 – As regards this criterion, the technical framework has not changed since the previous round of evaluation when Bulgaria was recommended to ensure full compliance with the term "funds" as defined under the TF Convention. The TF offence extends to "financial and other means" for which term no clear definition seems to be provided by law, and no reference on the legitimate or illegitimate source of funds is in place. There is no provision that would exclude the applicability of the TF offence to funds consisting of virtual assets.

While the Bulgarian legislation has remained the same, the respective FATF standards have since been raised (2017) so as to encompass not only "funds" but "funds and other assets" (including assets going beyond the concept of "funds" such as economic resources like oil and other natural resources). Likewise, there is no legislation in Bulgaria to meet this requirement.

Criterion 5.4 – The language of the TF offence does not require that the funds were actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act, with the notable exception of the financing collected or provided for an individual terrorist which, as discussed above, is at least indirectly linked to the commission of a concrete terrorist act.

Criterion 5.5 – For the reasons discussed under Criterion 3.8 above, this criterion can be regarded as being satisfied in the legal system of Bulgaria.

Criterion 5.6 – At the time of the previous assessment, the TF offence was punishable by imprisonment from 3 to 15 years and a fine up to BGN 30 000 (€15 343). In the meantime, however, the range of punishment was lowered to imprisonment of 3 to 12 years and the fine was removed, the reason for which changes is still unclear to the AT. While the current level of punishment can still be considered dissuasive, the removal of the possibility for an additional fine has made the available sanctions less proportionate.

Criterion 5.7 – See under c.3.10 (equally refers to corporate liability for ML and TF)

Criterion 5.8 – Attempt, participation, and complicity are generally covered by the Bulgarian CC as discussed under c.3.11 above. Organising or directing others to commit a TF offence can be categorized under the respective CC provisions either as participation/complicity or abetting (depending on whether the perpetrator also takes part in committing or attempting the TF offence) while c.5.8 (d) can either be subsumed under the categories mentioned above or considered as a *sui generis* preparatory act under Art. 110 of the CC.

Criterion 5.9 – All criminal offences, including the TF offence in Art. 108a (2) of the CC, can constitute a predicate offence for ML (see c.3.2).

Criterion 5.10 – The TF offence in Art. 108a (2) of the CC does not differentiate as to whether the terrorist financier should be in the same country or a different country from the one where the terrorist act occurred or will occur, or where the terrorists or terrorist organisations are located. The financing of extraterritorial activities, entities or individuals is thus implicitly covered by the TF offence, which was corroborated by prosecutorial jurisprudence already at the time of the 4th round assessment.

This conclusion is underpinned by general rules of the territorial and personal scope of the Bulgarian CC in Art. 3-6. These provide that the CC is applicable to any crimes committed in the territory of Bulgaria (a TF offence committed in Bulgaria is thus covered regardless of whether the funds went abroad) and to any crimes committed by Bulgarian citizens abroad (a TF offence committed abroad by a Bulgarian national is thus covered regardless of where the funds went). Even TF offences committed by foreigners abroad can be subsumed under Bulgarian jurisdiction if such crimes affect the interests of Bulgaria or Bulgarian citizens or where this is stipulated in an international agreement, to which Bulgaria is a party (such as the TF Convention itself).

Weighting and Conclusion

The TF offence has been amended to more comply with the FATF standards, but it still prescribes the purposive element for the TF offence, for all the offences, including the ones specified under the Conventions and Protocols listed in the Annex to the TF Convention. It is still unclear whether and to what extent the TF offence extends to funds and other assets as required by the FATF standards. Financing of travels to and from Bulgaria for the purpose of committing a terrorism-related act is not covered in its every aspect by the current legislation. The range of punishment for TF has been lowered and the elimination of additional fines reduced the proportionality of the sanctions. There is no corporate criminal liability and the administrative liability of legal persons for criminal offences is limited. Consequently, **R.5 is rated PC**.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 4th MER Bulgaria was rated PC with the former SRII. The summary of the factors underlying this rating were: (i) the procedures for amending the lists of designated entities was not without delay; (ii) the freezing did not extend to funds controlled, directly or indirectly by designated persons; (iii) deadlines for claiming the listing by third parties acting in good faith may impact the rights of *bona fide* third parties; and(iv) no specific guidance on freezing requirements was available for the private sector. Since then, Bulgaria made significant amendments to the Law on Measures Against the Financing of Terrorism (LMFT) with the aim of addressing the mentioned deficiencies. However, some shortcomings remain as described below.

Criterion 6.1 – At the EU level Bulgaria implements TFS pursuant to UNSCR 1267 and 1988 (on Afghanistan) – through Regulation (EU) 753/2011 and Council Decision 2011/486/CFSP and UNSCR 1267/1989 (on Al Qaeda) – through Regulation (EU) 881/2002 (and successors) and Council Decision 2016/1693/CFSP (replacing the Common Position 2002/402/CFSP. These Regulations have direct legal effect in Bulgaria.

(a) *(Met)* At a national level the MFA has the responsibility for proposing person or entities to the 1267/1989 and 1988 Committees. The MFA is the competent authority to purpose persons to relevant UN Committees by the virtue of the Rules on Organization of MFA (Art. 37). Bulgaria has not made any proposals for designations to date.

(b) *(Partly Met)* According to the Art. 4 of the LMFT, the SANS is the competent authority to collect, process, systematize, analyse, retain, use and provide information aimed at preventing and detecting actions by natural persons, legal persons, groups and organizations directed at financing of terrorism. However, Art. 4 makes no references to designation criteria set out in the relevant UNSCRs.

(c) – (e) *(Partly Met)* For these sub-criteria, Bulgarian Authorities claim that they would abide by the relevant UN 1267/1989 Sanctions Committee evidentiary standards, as well as follow the appropriate procedures, forms, and requests for information. These would include the EU Best Practices and FATF International best practices for TFS. However, there are no dedicated procedures in place.

Criterion 6.2

(a) At the EU level, the EU Council is responsible for deciding on the designation of persons or entities (Regulation 2580/2001 and Common Position 2001/931/CFSP). Within the context of Regulation 2580/2001 and Common Position 2001/931/CFSP, EU listing decisions shall be drawn up on the basis of precise information from a competent authority, meaning a judicial authority or equivalent of an EU Member State or third state. This does not include persons, groups and entities having their roots, main activities and objectives with the EU (EU internals).

At the national level, as per the Art. 5(1) of the LMFT the Council of Ministers, acting on a motion by the MFA, the MoI, the Chairperson of the SANS or the Prosecutor General, the Council of Ministers shall adopt, supplement and amend national lists both by their own motion and in case of a request of another country. However, the listing criteria as envisaged by the Art. 5(2) of the LMFT does not fully correspond to the specific criteria, as set forth in UNSCR 1373.

(b) At the EU level, identification of designation targets is covered by CP 2001/931/CFSP. At national level, as envisaged in Art. 5(1) of the LMFT the Council of Ministers acting on a motion by MFA, MoI, the Chairperson of the SANS or the Prosecutor General, adopts, supplements and amends national lists. However, as mentioned in the Criteria 6.2 (a), the listing criteria as envisaged by the Art. 5(2) of the LMFT does not fully correspond to the specific criteria, as set forth in UNSCR 1373.

(c) At the EU level the verification of the reasonable basis for any requests for designations received is handled by the 'Common Position 2001/931/CFSP on the application of specific measures to combat terrorism' Group (COMET Working Party) at the EU Council, which examines and evaluates the information to determine whether it meets the criteria set forth in UNSCR 1373. No clear time limit has been set for the WP's review. At national level, there is no set timeline and no mechanism to consider that the request is supported by reasonable grounds, or a reasonable basis to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373.

(d) At the EU level, as in case of c.6.2(c), the COMET WP assesses the existence of the designation criteria and other requirements under Common Position 2001/931/CFSP and makes decisions based on reliable and credible evidence without it being conditional on the existence of criminal proceeding. At the national level also, the decision of the Council of Ministers would be based on the existence of sufficient data, existence of criminal proceedings is not required.

(e) At the EU level there is no specific mechanism that would allow for requests to non-EU member countries to give effect to the EU list. At the national level the SANS and MoI are allowed to cooperate with competent foreign authorities as well as with international organisations for

the purpose of preventing and detecting actions by natural and legal persons directed at financing of terrorism. However, except for this general competency, there is no formalized procedure under which Bulgaria could ask another country to give effect to freezing measures with specific requirement to provide as much identifying information for designation as possible.

Criterion 6.3

(a) At EU level, all EU member states are required to provide each other with the widest possible range of police and judicial assistance on TFS matters, inform each other of any actions taken, cooperate and supply information to the relevant UNSC bodies (Art.8 Reg.881/2002; Art.8 Reg.2580/2001; Art.4 CP 2001/931/CFSP). At national level, according to the Art. 4 of LMFT the SANS collects or solicits the information for the purposes of preventing and detecting actions by natural persons, legal persons, groups and organizations that are directed at financing of terrorism to achieve the purpose of LMFT. At the same time deficiencies identified under 6.1 (b) and 6.2 (b) have cascading effect on this Criterion as well.

(b) At EU level, as for the UNSCRs 1267/1989 and 1988 regime, EU Regulation 1286/2009 provides for *ex parte* proceedings against a person or entity whose designation is considered. The Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the designation. At national level, no provision of the LMFT or other law requires that notice should be given to a party prior to a designation.

Criterion 6.4 – The EU procedure in respect of designations made by the relevant Committees of the UNSC implies a delay between the date of a designation by the UN and the date of its transposition into European law under Regulations 881/2002 and 753/2011 respectively, because of the time taken to consult between European Commission departments and translate the designation into all official EU languages. Thus, implementation of TFS pursuant to UNSCRs 1267/1989 and 1988, does not occur 'without delay' i.e., ideally within hours as required by the FATF standards. At national level Art. 5a of LMTF obliged the MFA to immediately publish on its website references to the adopted UNSCRs and successive designations. Upon publication, the obligation to freeze all funds or other assets immediately enters into force (LMFT Art. 4b (2)), thus fully addressing the TFS transposition delays at the national level. TFS related to UNSCR 1373, are implemented by European Council Regulations (Regulation 2580/2001) and are directly applicable in Bulgaria. These sanctions are thus implemented '*without delay*'.

Criterion 6.5 – The SANS and MOI are the competent authorities under the LMFT responsible for the implementation and enforcement of the TFS under the EU and national framework. Freezing obligations have been further stipulated under LMFT as follows:

(a) *(Met)* All natural and legal persons, including VASPS, in Bulgaria are required to freeze funds and other assets under UNSCRs 1267/1989 and 1988 only when such obligations have been transposed into the EU legal framework. As noted in c.6.4 such designations are transposed '*without delay',* through publication on the website of MFA, after which the obligation to freeze enters into force immediately.

Under UNSCR 1373, the obligation to freeze funds and other assets applies immediately in all EU member states because of the direct legal effect of the relevant EU instruments. However, under Council CP 2001/931/CFSP listed EU *'internals'* are not subject to freezing measures but only to increased police and judicial cooperation among members. Accordingly, the freezing without delay and without prior notice of the funds and other asserts of EU *'internals'* is a matter for

national law and policy. At the national level, as per the Art. 5(1) of LMFT the Council of Ministers, adopts, supplements and amends national lists based on the criteria set out in the Art. 5 (2) of the LMFT, which does not exclude EU internals. No provision of the LMFT or other law requires that notice should be given to a party prior to a freezing. The term funds or other assets is broadly defined under the Supplementary provisions § 1 (2) of LMFT, including also virtual assets, and it is line with the FATF definition.

(b) In relation to UNSCRs 1988 and 1267/1989, the freezing obligation as laid down in the EU Regulations extends to all funds or other assets defined in R.6, namely funds owned by designated persons (natural or legal) as well as funds controlled by them or by persons acting on their behalf, or on their order. These aspects are covered by the notion of 'control' in Art. 2 EU Regulation 881/2002, as amended by EU Regulation 363/2016, and Art. 3 EU Regulation 753/2011. For UNSCR 1373, the freezing obligation in EU regulation 2580/2001 (art.1(a) and art.2(1)(a)) applies to assets belonging to, owned or held by the designated individual or entity. It does not apply directly to funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. This gap is addressed in the Article 6 (1) and (4) of LMFT.

(c) At the EU level, and in a manner consistent with the UNSCRs, relevant Regulations prohibit EU nationals and persons within the EU making funds and other assets available to designated persons and entities. Provisions in national law does not precisely envisage that natural and legal persons should not make funds available directly or indirectly, wholly or jointly for the benefit of entities and persons owned or controlled directly or indirectly by designated persons and entities, as well as persons and entities acting on behalf of or at the direction of designated persons and entities.

(d) Designations decided at the EU level are published in the Official Journal of the EU and website and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures. At national level, the decision of the Council of Ministers concerning national lists is promulgated in the State Gazette immediately after adoption, as well as should be published on the web sites of the Council of Ministers, the MoI and the SANS. UNSCRs are published on the website of MFA immediately upon adoption. According to the Art. 5b of LMFT the SANS, together with MOI, issues instructions for the implementation of TFS. The website of MFA also contain links to the EU Best Practices for the effective implementation of restrictive measures and Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy. Besides, BNB also sends circulars to banks on updates of UNSCRs and the FID-SANS also conducts training focused on TFS implementation with all reporting entities.

(e) Natural and legal persons (including FIs/DNFBPs) are required to provide immediately to the designated national authority (SANS) any information about accounts and amounts frozen under EU legislation as per Art. 5.1 of EU Regulation 881/2002, Art. 4 of EU Regulation 2580/2001, and Art. 8 of EU Regulation 753/2011. At National level, Art. 9 (1) requires that any person who knows that certain operations or transactions are aimed at financing terrorism shall immediately notify the Minister of Interior and the Chairman of the State Agency for National Security. In addition, according to Art. 9 (3) of the LMFT FIs and DNFBPs under Art. 4 of the LMML (OEs under the AML/CFT legislation) shall also notify the FIU.

(f) The rights of *bona fide* third parties are protected at EU and national levels: Art. 6 Regulation 881/2002, Art. 7 Regulation 753/2011 and Art. 4 Regulation 2580/2001 and Art. 8 (5) of LMFT.

Criterion 6.6 – Bulgaria applies the following procedures for de-listing and unfreezing of funds or assets, including virtual assets of persons and entities no longer meeting the designation criteria:

(a) At EU level, there are procedures to seek de-listing through EU Regulations (EC Regulation 753/2011, Art. 11(4) for designations under UNSCR 1988 and EC Regulation 881/2002, art. 7a and 7b1 for UNSCR 1267/1989). At the national level however, no procedures exist with regard to submitting de-listing requests, although as stated by the authorities such requests are channeled to UN Committees through MFA.

(b) At EU level, for 1373 designations, the EU has de-listing procedures under Regulation 2580/2001. De-listing is immediately effective and may occur ad hoc or after mandatory 6-monthly reviews. At national level, Art. 5 (7) of the LMFT provides that MFA, the MoI, the Chairperson of the SANS or the Prosecutor General, acting on their own initiative or at the request of the parties concerned, submit a proposal to the Council of Ministers to remove a person from the list within 14 days after becoming aware of grounds of removal. The decision is promulgated in the State Gazette and published on the web sites of Council of Ministers, the Ministry of Interior, and the State Agency of National Security. Except for the legal provisions in LMFT, there are no publicly known procedures to request delisting on a national level.

(c) At the EU level, a listed individual or entity can write to the EU Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission Implementing Regulation, or a Council Implementing Regulation in Court, per Treaty on the Functioning of the European Union (TFEU) (Art. 263 (4)). Art. 275 also allows legal challenges of a relevant CFSP Decision. At the national level, the freezing decision can be appealed before the Supreme Administrative Court according to the Art. 5 (5) of LMFT. Except for the legal provisions in LMFT, there are no publicly known procedures to request to review designation decision on a national level.

(d) and (e) There are EU procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU (EC Regulation 753/2011, art.11; EC Regulation 881/2002, art.7a and 7e). At national level, no formal procedure exists to facilitate review by the 1988 Committee, as well as for informing persons and entities of the availability of the UN office of Ombudsmen. The only mechanisms existing is publication of a link on the MFA website.

(f) At the EU level, upon verification that the person/entity involved is not designated, the funds/assets must be unfrozen, according to EU Regulations 881/2002 and 2580/2001. At the national level, there is no explicit provision and procedures for unfreezing in the case of false positive. However, Articles 5 (5) and (6) of LMFT allows the affected persons to appeal before the Supreme Administrative Court under the procedure of the Administrative Procedure Code.

(g) At EU level, legal acts on delisting are published in the Official Journal of the EU and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission (EC Regulation 881/2002, Art.13; 753/2011, Art. 15; 2580/2011, Art.11). At national level, information on sanctions in force is to be published on the web sites of the Council of Ministers, the MoI, the SANS and the MFA according to the Art. 5a and 12 of LMFT. As envisaged by the Art. 5b of LMFT the SANS in coordination with the MOI issues instructions for

the implementation of TFS. However, this does not amount to providing guidance to FIs, other persons or entities, on their obligations with respect to delisting or unfreezing actions.

Criterion 6.7 – Both at the EU and national levels, there are procedures in place to authorize access to frozen funds or other assets, including virtual assets, which have been determined to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses: Art. 2a Regulation 881/2001, Art. 5 Regulation 753/2011, and Art. 5 and 6 Regulation 2580/2001, Art. 6 (5) and (6). At national level, the decision is determined on a case-by-case basis by the MoI.

Weighting and Conclusion

Main shortcomings are related to the following: (i) designation criteria set out in the relevant UNSCRs, are not described under the mechanism of identifying targets for designation; there is no dedicated procedures in place, to address requirements of Criterion 6.1 c)-e); (ii) the listing criteria as envisaged by the Art. 5(2) of LMFT do not fully correspond to the specific criteria, as set forth in UNSCR 1373; (iii) there is no set timeline and no mechanism to consider that the request is supported by reasonable grounds, or a reasonable basis to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373; (iv) there is no formalized procedure under which Bulgaria could ask another country to give effect to freezing measures; (v) there is no procedure in place with regard to submitting de-listing requests, as well as to facilitate review by the 1988 Committee, and informing persons and entities of the availability of the UN office of Ombudsmen; there is no guidance for FIs, other persons or entities, on their obligations with respect to delisting or unfreezing actions. **R.6 is rated PC**.

Recommendation 7 – Targeted financial sanctions related to proliferation

These requirements were added to the FATF Recommendations in 2012 and were therefore not previously assessed. Bulgaria primarily relies on EU legislation for the implementation of R.7. UNSCR 1718 concerning the DPRK is transposed into European law by Common Position 2006/795, Regulation 329/2007, and Council Decision 2013/183/CFSP. UNSCR 1737 concerning the Islamic Republic of Iran is transposed into European law by Regulation 267/2012 and Council Decision 2010/413. There is no national framework to address deficiencies in EU regulations.

Criterion 7.1 – R.7 requires the implementation of TFS without delay, meaning ideally within 24 hours. As described in criterion 6.4, there are delays in the transposition of UN designations into European law. Thus, implementation of TFS related to proliferation, does not occur 'without delay' i.e., ideally within hours as required by the FATF standards. As mentioned earlier, there is no national framework to address the delays. However, in practice in the case of targeted sanctions relating to proliferation, the risks are to some extent mitigated, because the EU applies sanctions to a larger number of entities that are not concerned by a UN designation, and in some cases is ahead of UN. As suggested by the authorities the Constitution, as well as the Act on International Agreements of the Republic of Bulgaria provide the possibility of direct implementation of PF related UNSCRs by Council of Minister`s decision. At the same, time it should be noted that the mentioned provisions are not used in practise (at least have not been during the evaluation period). The last Council of Ministers decision on UNSCR direct transposition was taken in 2012.

Criterion 7.2

(a) *(Not Met) At* the EU level, the EU Regulations require all natural and legal persons within or associated with EU to freeze the funds/other assets of designated persons/entities. This obligation is triggered as soon as the Regulation is approved and the designation published in the Official Journal of the European Union (OJEU) (EU Regulation 267/2012, Art. 49; Regulation 2017/1509, Art. 1). However, delays in transposing the UN designations into EU legal framework mean that freezing may not happen without delay for entities which are not already designated by the EU, and raises the question of whether the freezing action, in practice, takes place without prior notice to the designated person/entity. At national level, there is no requirement to freeze without delay and without prior notice, the funds or other assets of designated persons and entities.

(b) The freezing obligation under the EU framework extends to all types of funds and assets as required by c.7.2(b)(i)-(iv). This also includes virtual assets.

(c) The EU Regulations prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorized or notified in compliance with the relevant UN resolutions (Art. 6(2) Reg. 329/2007; Art. 23(3) Reg. 267/2012). The prohibition is wide enough and extends to VASPs as well.

(d) *Regulations* containing designations are published in the Official Journal of the EU. The EU also maintains a publicly available on-line consolidated list and has published Best Practices for the effective implementation of restrictive measures. The MFA provides links to the EU sanctions lists and to the EU Best Practices and Guidance papers on its website.

(e) All natural and legal persons must immediately provide all information that will facilitate observance of the EU regulations, including information about the frozen accounts and amounts, to the competent authority as indicated in the Annexes to the Regulations (Art. 10(1) Reg. 329/2007; Art. 40(1) Reg. 267/2012). In case of EU Regulation 267/2012, this is the SANS for Bulgaria. For the EU Regulation 329/2007 FIs are obliged, in case of dealings with FIs domiciled in the DPRK or their branches and agencies abroad, if they suspect or have good reason to suspect that funds are associated with PF, to quickly report to the FIU or to another competent authority (Art. 11a Reg. 329/2007). It is not clear which is the competent authority in case of Bulgaria. Attempted transactions are not precisely covered by the above-mentioned EU regulations.

(f) Regulations protect third parties acting in good faith (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) No 267/2012, art.42).

Criterion 7.3 – Under the EU Regulations 267/2012 (Art. 47) and 2017/1509 (Art. 55), EU Member States must take all necessary measures to implement EU regulations, which would include adopting measures to monitor compliance of the sanctions regime by FIs and DNFBPs. However, due to the absence of national framework for TFS related to proliferation, there are no sanctions available in case of non-compliance with obligations related to proliferation.

Criterion 7.4

(a) – (d) The EU Regulations contain procedures for submitting de-listing requests to the UN Security Council for designated persons or entities that, in the view of the EU, no longer meet the criteria for designation. The EU Council of Ministers communicates its designation decisions and the grounds for listing, to designated persons/entities, which have the right to comment on them, and to request a review of the decision by the Council. Such a request can be made regardless of

whether a de-listing request is made at the UN level (for example, through the Focal Point mechanism). Where the UN de-lists a person/entity, the EU amends the relevant EU Regulations accordingly. There are specific provisions for authorizing access to funds or other assets, where the competent authorities of Member States have 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. De-listing and unfreezing decisions taken in accordance with EU regulations are published in the EU Official Journal, the updated list of designated persons and entities is also published. The definition of Funds and other assets according to the Council Regulation (EU) No 267/2012 is broad enough and covers also virtual assets.

Criterion 7.5

(a) Interests or other earnings to frozen accounts or payments due under contracts, agreements or obligations are permitted, as long as they are subject to the freezing action (Art. 9 Reg. 329/2007; Art. 29 Reg. 267/2012). Since, there is no definition of interest or other earnings under EU regulations, the AT cannot conclude that virtual assets would precisely be covered.

(b) Payments due under a contract entered into prior to the date of listing are permitted provided that prior notification is made to the UN Sanctions Committee and that it is determined that the payment is not related to any of the prohibitions under the regulations (Art. 8 Reg. 329/2007; Art. 25 Reg. 267/2012). Since, there is no definition of payments due under a contract according to EU regulations, the AT cannot conclude that virtual assets would precisely be covered.

Weighting and Conclusion

Main deficiencies identified are related to the absence of national procedures for the implementation of TFS in relation to proliferation financing. **R.7 is rated PC**.

Recommendation 8 – Non-profit organisations

In its 2013 MER Bulgaria was rated LC with the old SRIII. The summary of the factors underlying this rating were: information on persons who own, control or direct the activities of NPOs was not kept within the NPOs. Since then, R.8 and its interpretive note were modified to ensure the applicability of risk-based approach in relation to NPOs.

Criterion 8.1

(a) In Bulgaria NPO sector is regulated through the Law on Non-profit Legal Persons (LNPLP), according to which NPOs are associations and foundations carrying out activities for the public benefit. According to the authorities all NPOs fall with the scope of FATF definition by virtue of legal definition. The NRA, in the analysis of specific TF channels, highlights religious organizations operating internationally as being more vulnerable to TF abuse and reflect the overall Bulgarian NPO sector with medium risk, based on observations and Bulgarian context in the period 2016-2019. At the same time, the analysis is not comprehensive (last comprehensive sectorial assessment was done in 2012) since it does not take into account activities, basic features and other contextual information on the sector (such as analysis of donors, founders of NPOs, donations and main directions of disbursements, any connections with high risk or conflict zones, transactional data and etc).

(b) Bulgaria has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors could abuse those NPOs.

(c) Several legislative changes were made to ensure the flexibility of legal obligations for NPOs as obliged entities, as well as introducing some elements of risk-based approach. In 2016 legislative

changes were made in LNPLP to strengthen administrative sanctioning mechanism of NPOs that are subject to TFS or are reasonably believed to be carrying out activity in furtherance of terrorism. At the same time, a formal review to assess the adequacy of measures in relation to those types of NPOs which are vulnerable to TF abuse was not conducted.

(d) There is no specific requirement to periodically re-assess the NPO sector. The only provision in this respect refers to the NRA which shall be updated every two years to identify, assess, understand and mitigate the risks of money laundering and the financing of terrorism for the purposes of LMML and LMFT. This per se would also include NPO risk assessment.

Criterion 8.2

(a) Bulgaria has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs. The LNPLP sets the prerequisites for the foundation, the organization, financial management, and the dissolution of an association/foundation. Besides, NPOs operating in the country have annual reporting obligations. As envisaged in the Art. 6 (1) of LNPLP the legal capacity of NPOs originates from their registration in the register of non-profit legal persons (Art. 6, para 1 of the LNPLP). The register is kept by the Registry Agency to the Minister of Justice (Art. 17 of the LNPLP). According to the Art 38 (1) (2) of the Law on Accountancy the NPOs are obliged to publish their annual financial statements, consolidated financial statements and annual reports. Besides, NPOs operating for public benefit are also subject to statutory independent financial audit (Art. 37).

(b) *NPOs* are OEs under the Bulgarian legal framework. The outreach undertaken is not focused on potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks but is broader and includes general obligations under the AML/CFT legislation. In the period August - September 2020 the Bulgarian Centre for Non-Profit Law with the support of FID-SANS organized 4 workshops and consultations for NPOs with regard to AML/CFT matters, including measures that would protect NPOs from TF abuse. No dedicated outreach was provided to the donor community, except for 1 workshop, in which some representatives from donor community also took part. At the same time, the online availability of the NRA outcomes as well as other information regarding the NPOs (through the Commercial Register and Register for non-profit legal) provide access of the donor community to relevant materials and to some extent mitigate the fact that no dedicated outreach was provided to the donor community.

(c) FID-SANS together with the Bulgarian Centre for Non-Profit Law developed a Methodology and Criteria for Risk Assessment for NPOs, which is considered to be a useful tool helping NPOs to identify, understand and assess the risk of their activity being used for the purpose of ML/TF. The cooperation with BCNL included also other areas, such as capacity building within NPO sector, identification of BOs, which would per se in general also address TF risks and vulnerabilities.

(d) According to the Art. 3 of the Law on Limitation of Cash Payments, payments in the territory of Bulgaria shall be made only via bank transfers or deposits to payment accounts when the value of the payment is equal or in excess of 10000 BGN (app. 5000 Euros), as well as linked payments below the mentioned amount if total value is equal to or exceeds BGN 10,000.

Criterion 8.3

NPOs are OEs according to the Art. 4(28) of LMML with limited obligations under the LMML. FID-SANS is the competent authority to supervise and monitor the level of implementation the relevant requirements by NPOs. Besides, NPOs are required to be registered, maintain accounting information, publish reports and etc. According to the Art. 78(1) of the Accounting Act, the National Revenue Agency monitors the compliance with the accountability requirements. However, it should be noted that all of the measures described above (with some exceptions, namely, conducting risk assessment according to LMML based on the annual turnover, which, however, does not relate to TF risk) are applied regardless of TF risk to all NPOs operating in the country.

Criterion 8.4

(a) FID-SANS is the competent authority to supervise and monitor the level of compliance of NPOs with the relevant requirements. In addition, the National Revenue Agency monitors the compliance with the accountability requirements. However, as noted under Cr. 8.3 the supervision/monitoring towards NPOs is not risk based and applies to all NPOs regardless of TF risk.

(b) NPOs are obliged persons. Thus, the sanctions as envisaged by the LMML apply to them, as well as persons acting on their behalf. A number of sanctions are available for NPOs as well as persons acting on their behalf (For more information regarding sanctions for breaches of AML/CFT related obligations please see R35). As regards to other obligations sanctions available are as follows: Under the Law on the Commercial Register and the Non-Profit Legal Entities Register breaches of registration requirements are liable to fines (app. 250-500EUR). In addition, the National Revenue Agency applies sanctions for breaches of the Accounting Act, particularly in relation to submitting and publishing financial statements (app. 250-1500EUR). Moreover, NPOs may also be dissolved in case they are listed under Art. 5 of LMFT.

Criterion 8.5

(a) There are mechanisms in place for co-operation, co-ordination and information sharing with regard to combatting terrorism financing as envisaged in the LMFT. The SANS and FID-SANS play vital roles in these processes. The mentioned mechanisms would per se include also co-operation, co-ordination and information sharing in respect of NPOs. Besides, the information contained in the Register of non-profit legal entities is also public.

(b) The investigation of terrorism-related offences (including TF), including NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations is the responsibility of and ensured by the following authorities: the State Agency for National Security (pre-investigative stage) and the Ministry of Interior (investigative stage). The latter have the wide range investigative expertise and capability to examine also NPOs at stake.

(c) Full information on the administration and management of NPOs is accessible in a timely manner, given that relevant information is stored publicly and is easily accessible through the Register of Non-Profit Legal Persons. The access to financial and programmatic information not contained in the Register of Non-Profit Legal persons and is regulated under CCP (please refer to R. 9 and 31).

(d) Bulgaria has in place a legal framework to ensure that information is shared between competent authorities. According to Art. 9 of LMFT any person, including state bodies, who knows that given financial operations or transactions are intended to finance terrorism, shall be obliged to notify immediately the MoI and the Chairperson of the SANS. In addition, Art. 9a of LMFT envisages that supervisory authorities provide information on any findings related to terrorism financing to the MoI and SANS immediately, as well as FID-SANS and vice versa.

Criterion 8.6 – Bulgaria uses the general procedures and mechanisms for international cooperation to handle requests relating to NPOs. International requests for information regarding particular NPOs that are suspected of TF or other forms of terrorist support are dealt with by MOJ in the case of MLAs or the FID-SANS in the case of requests received from other FIUs. Besides, all LEAS may also rapidly exchange information with their counterparties through International Operational Cooperation Directorate (IOCD) of the Ministry of Interior and vice versa.

Weighting and Conclusion

Bulgaria fully or mostly meets most of the criteria under R.8., The remaining deficiencies are following: (i) Bulgaria did not conduct comprehensive analysis of NPO sector recently (last complex analysis was conducted in 2012); (ii) Bulgaria has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors could abuse those NPOs; (iii) No dedicated outreach was provided to the donor community; (iv) the monitoring or supervisory measures are applied to all NPOs regardless of TF risk and are not risk based. The AT considers the remaining deficiencies as serious having negative impact on compliance of Bulgaria with R.8. these deficiencies have been given more significant weight when determining the final rating of this recommendation. **R.8 is rated PC**.

Recommendation 9 – Financial institution secrecy laws

In the 2013 MER, Bulgaria was rated compliant with former R.4.

Criterion 9.1 – The requirement of this criterion is addressed through several legal acts – the LMML, LMTF, RILSANS, LCI, LPSPS, LBNB.

The FID-SANS is able to access information held by FIs/DNFBPs for the purpose of its key FIU functions outlined in the LMML: (1) the FID-SANS has powers in relation to its performance of supervisory functions under Art. 109-111 of the LMML, most notably that the provision of documents, information, references, excerpts, written and oral explanations for the purposes of the inspections referred to in the LMML; (2) the FID-SANS has additional powers in Art. 74(1) to request information about suspicious operations, transactions or customers from FIs/DNFBPs with the exception of the BNB and credit institutions which pursue business in the territory of Bulgaria and to instruct FIs/DNFBPs to monitor transactions and inform the FID-SANS on these. However, the BNB and credit institutions are covered under Art. 74(2) of the LMML, which grants necessary powers to the FID-SANS to request above mentioned information upon written notification. The combination of Art. 74 of the LMML and Art. 9(3) and (6) of the LMFT does not allow information to be refused on the basis that it is covered by official, banking, trade or professional secrecy, constitutes tax and insurance information or protected personal information.

Art. 90(1) of the LMML allows the FID-SANS acting on its own initiative and on request to exchange information about a suspicion of money laundering and about associated predicate offences with the relevant international authorities, authorities of the EU and authorities of other

countries on the basis of international treaties and/ or by reciprocity. Similarly, based on Art. 14(2) of the LMFT, this is also relevant for TF-related information.

In respect of the BNB, Art. 87 (11) of LCI provide requirements for FIs to provide information and documents to the BNB in relation to its functions and the powers of banking supervision authorities for banks. Art.159 of the LPSPS is also relevant for payment service providers.

In respect of the FSC, Art. 18, Art. 19(5) of the FSCA along with Art. 24, 25(7) and (11) of the LFSC allows the FSC to access all types of information held by OEs as well as information from third parties to conduct cross-checks for the purposes of the performance of its supervisory functions.

In respect of the NaRA, the powers of the revenue authorities stipulated in Art. 12 of the Tax and Social Security Procedure Code include: access to premises, documents, right to carry out all kinds of inspections, to demand explanations, etc. In addition, as noted under c.27.4 (see R.27), only the FID-SANS and the BNB has the powers to compel information required for supervision with the LMFT.

In respect of information sharing between competent authorities domestically, the AT was informed that the relevant sectorial legislation provides for the power and obligation for each authority to collect and exchange information with other authorities, however, no legal provisions have been provided to ascertain this. The LMML (Art. 87) covers provision of ML and TF related information by the FSC and the BNB to the FID-SANS only.

In respect of information sharing by the supervisory authorities (other than FID-SANS) with their foreign counterparts, only the FSC and BNB can cooperate with the foreign counterparts, however, the scope of cooperation demonstrates significant shortcomings, please see c.40.12 for more information. No legal provisions exist on information sharing with foreign counterparts by other supervisory authorities (NaRA, CRC).

In respect of sharing information between financial institutions, Art. 80 (3) and (5) of the LMML allows information sharing between FIs (exception being PMOs, leasing undertakings, pension insurance) and in a FI group in cases relating to the same customer and the same transaction involving two or more parties.

Data and documents held by the FIs can be requested by virtue of Art. 159 (1) of the CPC while information covered by bank secrecy can be obtained by an order issued by the competent district court pursuant to Art. 62 (6) of the LCI.

Deficiencies relating to the services exempted from the regulatory environment apply here, i.e., licensing and supervisory regime does not cover safekeeping services, payment services related to paper-based vouchers and paper-based traveller's cheques (except when they are provided by banks), and certain VASP activities. See R.26 and R.15 for more information. This might hinder the competent authorities' ability to access relevant information held by certain persons that provide activities falling outside the regulatory scope.

Weighting and Conclusion

Bulgaria has following deficiencies under R.9: (i) information exchange domestically is limited in scope; as well as international exchange of information by the supervisors (other than the FID-SANS) with the foreign counterparts (ii) deficiencies exist in relation to the ability to request information in all circumstances and particularly in relation to TF and due to some financial and virtual assets related activities that fall outside the regulatory scope. Consequently, **R.9 is rated LC.**

Recommendation 10 – Customer due diligence

In the 2013 MER, Bulgaria was rated LC with former R.5. The assessment identified technical deficiencies related to the definition of "beneficial ownership" and the application of simplified CDD measures.

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime, does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 10.1 – The preventative measures of the LMML apply to "*obliged entities*", which are defined at Art. 4 of the LMML and include both FIs and DNFBPs. Art. 18 of the LMML prohibits OEs from opening anonymous accounts or accounts in obviously fictitious names.

Criterion 10.2 – Art. 11 of the LMML requires OEs to apply CDD in the following circumstances: when establishing a business relationship; when carrying out an occasional transaction (i.e., a single or several linked transactions) amounting to EUR 5 000 or above when effected in cash, EUR 1 000 or above when the transaction constitutes a transfer of funds as defined under Regulation (EU) 2015/847 or EUR 15 000 or above in other circumstances.

Since 2012, the LCPA has prohibited the use of cash for transactions equal to or exceeding BGN 10 000 except in limited scenarios. The CDD requirements regarding cash also apply in cases where the OE could not have known at the time that the transaction would have exceeded the threshold permitted.

Art. 14 of the LMML requires OEs to apply CDD where there is a suspicion of ML regardless of any exemptions or thresholds for CDD. There is no explicit requirement to apply CDD where there is suspicion of TF, however, this shortcoming is partly mitigated by Art. 9(2) of the LMFT that states that CDD measures shall be applied "*with a view to preventing the use of the financial system for the purposes of terrorist financing*".

Art. 15 of the LMML requires OEs to identify and verify the identity of the customer and the beneficial owner (that does not constitute full CDD) where information is insufficient for CDD purposes and where doubt arises about the veracity, correctness or adequacy of identification data. Further, Art. 16 of the LMML requires OEs to keep the information collected through all due diligence measures up to date.

Criterion 10.3 – Art. 10 of the LMML states that CDD, as applied to business relationships and occasional transactions under Art. 11, shall include identifying the customer and verification of the identity using documents, data or information obtained from reliable and independent sources.

The term "*customer*" is defined in §1 of the LMML as a "*natural or legal person or other legal entity*". The term "*other legal entity*" is also defined and includes legal arrangements.

Section V of Chapter Two of the LMML mandates the requirements regarding the identification and verification of customers. Art. 53(7) includes that, where identification takes place without the presence of the natural person, verification of the identification data (which includes photographic identification) shall be verified according to the procedure established by Art. 55(2). Furthermore, Art. 53(8) states that verification may be carried out by means of electronic identification. Art. 55(2) requires two or more of methods to be utilised for remote verification. Methods include "*technical means to authenticate the veracity of the presented documents"* and

"another method" which gives the OE "reason to consider that the customer has been duly identified". This seemingly allows for a wide variety of practical verification measures, including video calls which are subject to further requirements at Art. 41 of the RILMML.

Criterion 10.4 – Art. 65(1) of the LMML requires OEs to establish the identity of both the customer and the third party in circumstances where a third-party acts for the customer and to obtain proof of the powers of representation. Although there is no explicit requirement to verify the identity of a person who is authorised to act on behalf of a client, Art. 40 of the RILMML does require, in cases where an operation or transaction is conducted via a third party, to identify and verify the third party.

Art. 65(2) of the LMML regulates cases where operation or transaction to be carried out on behalf of and/or for the account of a third party without authorisation, provided that the person who carried out the operation/transaction and a third party on whose behalf this person acted are both identified and verified. The possibility to carry out operations and transactions on behalf of a client without authorisation goes against the requirements under the FATF standard and the common principles governing contractual arrangements between persons. The AT is advised by the authorities that "*without authorisation*" refers to cases where the persons is permitted to act on behalf of the customer by law rather than by authorisation by the customer, however, these country statements cannot be proven, as Art. 65(2) of the LMML does not provide for the circumstances under which customer is allowed to carry out operations on behalf of the third party without authorisation, nor make any reference to other legal acts or provisions of the same legal act. The shortcoming is mitigated to some extent regarding payment services as the BNB's Ordinance No.3 on the Terms and Procedure for Opening Payment Accounts, Executing Payment Transactions and Using Payment Instruments establishes that activities may be conducted on behalf of a customer where there is a notarized letter of attorney.

Art. 54 of the LMML requires OEs to identify the legal representatives of a customer that is a legal person or other legal entity, and Art. 55 requires verification of that identity through the measures prescribed which constitute independent, reliable sources.

Criterion 10.5 – Art. 10 of the LMML states that CDD shall include identifying and taking reasonable measures to verify the identity of the beneficial owner of a customer. Articles 59-62 of the LMML prescribe methods for establishing beneficial ownership which constitute independent, reliable sources. Art. 55 (1) item 2 of the LMML requires OE to remove any doubt as to who the beneficial owner is. The term "*beneficial owner*" is defined in § 2(1) of the Supplementary Provisions of the LMML as any natural person or persons who ultimately owns or controls a legal person or other legal entity, and/or any natural person or persons on whose behalf and/or for whose account an operation, transaction or activity is being conducted.

Criterion 10.6 – Art. 53(3) of the LMML requires OEs, when entering into a business relationship with a natural person, to collect data relating to the person's professional activities and the purpose and nature of the involvement of the person in the business relationship. Such data must be collected from documents, data or information from reliable and independent sources. Art.54(4) of the LMML requires to collect data on the client, who is a legal person or arrangement, the scope of activity and the purpose and nature of the business relationship or of the occasional operation or transaction. Whilst there is no explicit requirement to "*understand*" the purpose and nature of the business relationship as opposed to "*collect data*" the requirement is met at Art. 10(3), which does require "assessment" of such information.

Criterion 10.7 – Art. 10(5) of the LMML requires OEs to verify transactions undertaken throughout the course of a business relationship to ensure that the transactions are consistent with the risk profile of the customer and with information collected for CDD purposes. The LMML requires OEs to "*verify*" transactions rather than to "*scrutinize*" and there is no explicit requirement to ensure that transactions are consistent with the OE's knowledge of the customer and its business. However, this shortcoming is partly mitigated by the provisions of Art. 21 of the RILMML that require OEs to take into consideration how transactions "*relate to the nature and purpose of the business relationship or occasional transactions or operation*" and when performing risk assessment, the OEs are required to check whether "*operations are consistent with the risk profile of the customer and with the information collected*". Mitigation is considered partial as these requirements apply to conducting risk assessment rather than throughout the course of the relationship and transaction monitoring.

The checks on the source of funds, according to Art. 10(4) of the LMML are applicable "*in the cases provided for in the law"* and thus are only explicitly required in circumstances related to PEPs and high risk third countries (Art. 39 and Art. 46 of the LMML). Otherwise, the requirement is inferred but not explicit; There is no clear requirement to conduct the checks on the source of funds as part of standard CDD, however, Art. 25(3) item 6 states that for simplified CDD, the source of funds may be assumed.

Art. 10(5) of the LMML requires timely updating of the documents, data and information collected. Requirements under Art. 16(1-2) further stipulate that information collected through CDD measures shall be periodically reviewed and, where necessary, databases and customer dossiers shall be updated. The databases and customer dossiers and business relationships which are higher risk shall be reviewed and updated at shorter intervals. However, the legislation does not make an explicit requirement that the CDD information, data and documents shall be kept "*relevant*". This shortcoming is partly mitigated as banks, payment institutions and e-money institutions are required to comply with EBA Risk Factor Guidelines which include a requirement to scrutinise CDD.

Criterion 10.8 – Art. 10(2) of the LMML requires OEs to take appropriate measures to understand the ownership and control structure of the customer. Art. 54(3) of the LMML requires OEs, when identifying legal persons and legal arrangements, to identify the structure of the ownership, management and control of the customer and, under Art. 54(4)(6), to collect data on the scope of the activity and nature of the business relationship or occasional transaction. However, there is no explicit requirement to *"understand"* the nature of the customer's business. This shortcoming is partly mitigated as banks, payment institutions and e-money institutions are required to comply with EBA Risk Factor Guidelines which include a requirement to "understand".

Criterion 10.9 – Art. 54 of the LMML requires OEs to identify customers that are legal persons or other legal entities and verify this information through the presentation of original or notarised copies of extracts of relevant registers and of the memorandum of association, constituent instrument or other documents necessary to establish the required data. The data, according to Art. 54(4) of the LMML, includes the name and legal form of the entity, location of head office, registered address, correspondence address and principal place of business, and information on management and control bodies. This does not fully satisfy the requirement of the sub-criterion 10.9(b), under which OEs should be required to verify the identity of the customer that is a legal person or legal arrangement including by obtaining names of the relevant persons having senior management positions (i.e., names of position holders as opposed to information on management and control bodies).

Art. 54(2) of the LMML provides for an alternative method to obtain original or notified documents relating to customers that are legal persons and are established in EU Member States. In this case, certain OEs are allowed to identify legal persons by means of reference to the record of the legal person in the commercial register or in the relevant public register and by documenting the identification actions taken. This approach is not in line with the FATF standard that requires to both identify and verify the identity (i.e., a two-step process) of the customer. Moreover, it might have negative implications on practical implementation in the circumstances where information contained in the public registers is not up to date.

Art. 54(7) of the LMML requires the identification of natural persons that are the legal representatives of a customer that is a legal person or other legal entity.

Criterion 10.10 – Art. 10 of the LMML requires OEs to identify and take reasonable measures to verify the identity of the beneficial owners of customers.

§ 2(1) of the Supplementary Provisions of the LMML defines "*beneficial owner*" as any natural person(s) who ultimately owns or controls a legal person or other legal entity or on whose behalf activity is conducted, subject to conditions regarding ownership and voting rights and separate stipulations regarding trusts and foundations.

(a) The BO definition states that, in the case of corporate legal persons and other legal entities, this shall be the person with direct or indirect ownership of a sufficient percentage of the shares, ownership interest or voting rights or control via other means. Persons holding at least 25 per cent ownership interest are considered beneficial owners.

(b) The BO definition includes that BO is also a person who exercise control via other means. Control is defined within the meaning given by paragraph 1c of the Supplementary Provisions of the Commerce Act, as well as any opportunity which, without being an indication of direct or indirect ownership, confers the possibility of exercising decisive influence on a legal person or other legal entity in the decision-making process for determining the *composition* of the bodies responsible for the management and supervision, the transformation of the legal person, "*the cessation of the activity thereof and other matters essential for the activity thereof. In addition, exercising ultimate effective control over a legal person or other legal entity by means of exercising rights through third parties conferred, inter alia, by virtue of authorisation, contract or another type of transaction, as well as through other legal forms conferring the possibility of exercising decisive influence through third parties, shall be an indication of "indirect control"".*

The LMML does not explicitly state that an OE must identify and take reasonable measure to verify the identity of a natural person who exercises control through other means than ownership in the circumstances included within c.10.1, where (a) there is doubt that a person with the controlling ownership interest is a beneficial owner or (b) no natural person is found who exercises control through ownership interest. However, this shortcoming is partly mitigated by the requirements of the Art. 59 (1) (2) of the LMML that requires OE to remove any doubt as to who the beneficial owner is.

(c) The BO definition includes that, where no BO (BO in the meaning of a person who either beneficially owns by holding certain percentage of shares or exercising control via other means) is identified, the natural person who holds the position of senior managing official shall be regarded as the BO.

Criterion 10.11 – The BO definition at § 2of the LMML includes that, in the case of trusts, escrow funds, foundations and other similar foreign legal arrangements, the BO shall be the settlor,

trustee, protector (if any), beneficiaries or class of beneficiaries, person in whose main interest the arrangement is established and any other person exercising ultimate effective control. Art. 10 of the LMML requires OEs to identify and take reasonable measures to verify the identity of the beneficial owners of customers. In addition, Art. 54 sets out legal measures for the identification and verification for legal persons, please see c.10.9 for more information.

Criterion 10.12 – Art. 19(1) of the LMML requires insurers and insurance intermediaries to identify beneficiaries that are specifically named persons (meaning either natural or legal persons) or other legal entities that are named at the time of entering into contract; verification of beneficiaries shall take place at the time of or before the pay-out or at the time of or before the beneficiary intends to exercise its rights to payments conferred under the insurance contract. The same is applicable to beneficiaries that are designated by characteristics, by class or by other means. In both cases, verification must occur prior to payment.

Criterion 10.13 – There is no explicit requirement in the LMML to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable for reasons other than being identified as a PEP. In addition, the LMML is silent on the circumstances, when, upon determination that a beneficiary who is a legal person or legal arrangement presents a higher risk, OE should be required to take enhanced measures. Although authorities advised that, when assessing risks related to beneficiaries, general rules of risk profiling and, linked to this, scope of CDD which is dependent on risks, are applicable, however, this is not relevant for the purpose of complying with a very specific requirement under c.10.13 aimed at targeting beneficiaries of life insurance policies. Art. 22 of the RILMML requires OEs to comply with EBA Guidelines of ML/TF Risk Factors which includes, at Chapter 7 (Sectoral guidelines for life insurance undertakings) factors that *may* constitute higher risk and where enhanced CDD *may* be appropriate. However, this does not explicitly require neither risk assessment nor enhanced CDD.

Criterion 10.14 – Art. 15(1) of the LMML requires OEs to identify and verify the identity of the customer and BO(s) before the establishment of a business relationship, the opening of an account or carrying out of an occasional transaction, where applicable.

Art. 21 of the LMML allows for the verification of identity to be completed during the establishment of a business relationship (but not after it) provided that certain conditions are met: (1) the completion of the verification before the establishment of a business relationship, in view of the nature of the said relationship, objectively leads to an interruption of the normal conduct of the activity concerned; (2) there is low risk of ML/TF and measures have been taken to effectively manage the risks; (3) the verification must be completed as soon as possible after initial contact with the customer.

Art. 22 of the LMML allows for a credit institution and certain investment businesses to open an account prior to the verification of identity on condition that no operations or transactions may occur prior to verification.

In addition, Art. 25(2) of the LMML allows for verification of customer identity to be completed after establishing a business relationship as part of simplified CDD measures if risk-mitigating conditions are present.

Criterion 10.15 – There is no explicit requirement for OEs to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification under Art. 22 of the LMML, however, risk is managed by prohibiting operations or

transactions prior to verification. Art. 25, under which simplified due diligence is allowed, also requires risk-mitigating conditions to be present.

Criterion 10.16 – Art. 16 of the LMML requires CDD information to be periodically reviewed and, where necessary, updated. More frequent reviews are required for higher risk customers. Art. 15(2) of the LMML requires OEs to carry out CDD measures where there are doubts about the veracity, correctness or adequacy of identification data and in the event of a change in that data. As well as the general requirement to review CDD information, as described above, there exists an overarching requirement at Art. 98(9) to apply all LMML measures on the basis of conducted risk assessments. There is, however, no explicit requirement (1) to take into account materiality and varying risks levels (except for higher risk customers and relationship) and (2) conduct due diligence at appropriate times, taking into account whether and when CDD measures have been previously undertaken and the adequacy of data obtained, including ensuring that CDD for existing customers is in accordance with the current legislation.

Criterion 10.17 – Art. 35 of the LMML requires OEs to carry out enhanced CDD measures in high-risk scenarios as listed, which include conducting activity with PEPs, persons in high-risk third countries, products with high levels of anonymity, new and high-risk products, business practices and delivery mechanisms or technologies, unusual activity, correspondent relationships with a third-country credit or financial institution and all other cases identified as high risk (under Chapter Seven of the LMML) by the OEs through business wide ML/TF risk assessments, national or sectorial risk assessments..

Criterion 10.18 – Section III of the LMML deals with simplified CDD. Art. 25 of the LMML states that simplified CDD measures may be carried out depending on the assessment of the potential risk subject to various conditions that are stipulated in Art. 26. Simplified measures include identifying customers without the need to take copies of identification documents, verifying the customer's identity after establishing a business relationship, adjusting the frequency of CDD and ongoing monitoring and making assumptions regarding the purpose and nature of the business relationship and of the source of funds.

Art. 26 of the LMML lists conditions for use of simplified CDD measures including that the measures must be approved by the senior management of the OE and that prior notification of the use of simplified measures is provided to the FID-SANS.

Art. 28 of the LMML allows for simplified CDD measures to be carried out where the customer is a central or local authority in Bulgaria provided that the general conditions of Art. 26 are met which includes that the activity is not identified as medium or high risk in the NRA and is identified as low risk by the OE.

Criterion 10.19 – In cases where the OE is unable to comply with the CDD requirements, Art. 17 of the LMML requires that a transaction or establishment of a business relationship is not carried out, and, in the case of an existing business relationship, that the relationship be terminated. The exception to this is private enforcement agents (which do not constitute an FI or DNFBP under FATF Standards) as their function includes the execution of court decisions. Art. 17(5) further requires the OE to consider making a disclosure to the FID-SANS regarding knowledge or suspicion of ML. There is no explicit requirement to consider making a disclosure regarding knowledge or suspicion of TF. However, Art. 9(2) of the LMFT states that CDD measures shall be applied "*with a view to preventing the use of the financial system for the purposes of terrorist financing*".

Criterion 10.20 – There is no legal provision to permit an OE not to complete CDD in cases where there is a ML/TF suspicion and reasonable belief that performing the CDD process will tip-off the customer.

Weighting and Conclusion

The following **minor shortcomings** have been identified: there are no explicit requirements (i) to apply CDD where there is suspicion of TF (c.10.2); (ii) to carry out CDD other than identification and verification of identity where doubt arises regarding identity data (c.10.2); (iii) to verify the identity of a person acting on behalf of a customer and no legal provisions regarding cases where third parties are permitted to act without authorisation (c.10.4); (iv) to keep CDD "*relevant*" and to ensure that transactions are consistent with the OE's knowledge of the customer and its business(10.7); (v) to do checks on source of funds apply except in relation to PEPs and high risk third countries (c.10.7); (vi) understand the nature of the customer's business (c.10.8); (vii) to identify and take reasonable measure to verify the identity of a natural person who exercises control through other means than ownership in some circumstances (c.10.10); (viii) there are no explicit requirements to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable for reasons other than being identified as a PEP (c.10.13); (ix) to adopt risk management procedures concerning conditions under which a customer may utilise the business relationship prior to verification (c.10.15); (x) to take into account materiality and varying risks levels (except for higher risk customers and relationship) (c.10.16); (xi) to conduct due diligence at appropriate times, taking whether and when CDD measures have been previously undertaken and the adequacy of data obtained (c.10.16); (xii) to consider making a disclosure regarding TF (c.10.19).

In addition, the following shortcomings are considered **moderately severe** in light of the context of Bulgaria, namely use of legal persons and strawmen in ML schemes as well as issues relating to nominees and bearer shares: (i) the legislation allows for an operation or transaction to be carried out on behalf of and/or for the account of a third party without authorisation (c.10.4); (ii) the legislation allows for an alternative method to identify and verify the legal persons and arrangements, i.e., it is permitted not to request certified identity documents from the legal persons provided that legal personality information can be obtained from the EU registers (c.10.9); (iii) there are no requirements to verify the names of the relevant persons having senior management positions in the legal person or legal arrangement (c.10.9).

Furthermore, the following **severe** shortcoming was identified: there are no legal provisions to permit an OE not to complete CDD in cases where there is a ML/TF suspicion and reasonable belief that performing the CDD process will tip-off the customer (c.10.20).

Deficiencies relating to the financial services exempted from the regulatory environment are also relevant here.

R.10 is rated PC.

Recommendation 11 – Record-keeping

In the 2013 MER, Bulgaria was rated PC with old R.10. The assessment identified technical deficiencies related to the lack of requirement to keep transaction records that applies to all FIs; no provision to ensure that transaction records should be sufficient to permit reconstruction of individual transactions to be maintained and having no provision for entities to keep records longer than 5 years when requested to do so by a competent authority.

According to the analysis of the 1st Compliance Report of Bulgaria[108], the authorities had taken steps to address the identified deficiencies under R.10. In particular, the necessary amendments had been brought to the LMML and to the RILMML. Based on these measures the report concludes that the rating was brought to a level equivalent to "LC".

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime, does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 11.1 – Art. 67(1-2) of the LMML requires OEs to maintain all documents, data and information obtained under the LMML and the RILMML for a period of at least 5 years from when a transaction or operation is carried out. Further detail regarding transaction data to be kept is provided in the LCI (Art. 67(4-6)) and the LPSPS (Art. 76(1)(3), Art. 124). No distinction is made between domestic and foreign transactions therefore the requirements apply to both equally.

Criterion 11.2 – Art. 67 of the LMML adequately requires OEs to maintain all documents, data and information collected and prepared in accordance with the LMML and the RILMML, thereby addressing the requirement to maintain account files, business correspondence and results of analysis.

CDD records must be kept for a period of at least 5 years from when an occasional transaction or operation is carried out or from when a business relationship is terminated.

Criterion 11.3 – Art. 69 of the LMML requires the information, documents and data on individual transactions and operations to be retained in such a way as to allow the timely recovery of said information to be made available as evidence in judicial and pre-trial proceedings.

Criterion 11.4 Art. 68(1) of the LMML requires that all documents, data and information collected and prepared according to the procedure established by the LMML and the RILMML shall be retained so as to be available to the FID-SANS, to the relevant supervisory authorities and to auditors. Art. 68(1) of the LMML requires that the said documents, data and information shall be provided to the FID-SANS upon request, in the original, an officially certified duplicate copy, excerpt or reference within a time limit and in a format determined by the Director of the FID-SANS. Art. 109 of the LMML grants the right for other supervisory authorities to require copies of the documents when carrying out onsite examinations and other supervisory duties; Art. 110 and 114(2) of the LMML obliges OEs to cooperate with the supervisory authorities on this matter and provide all necessary documents within a time limit and in a format determined by the supervisory authorities.

Weighting and Conclusion

Deficiencies relating to the financial services exempted from the regulatory environment are relevant here.

R. 11 is rated LC.

[108] Bulgaria 1st Compliance Report, 3 July 2018. Available at https://www.coe.int/en/web/moneyval/jurisdictions/bulgaria

Recommendation 12 – Politically exposed persons

In the 2013 MER, Bulgaria was rated LC with former R.6. The assessment identified technical deficiencies related to the scope of the PEP definition and lack of requirement for senior management approvals when entering into and maintaining business relationship with PEPs.

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime, does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 12.1 – Art. 36(1) of the LMML requires OEs to apply enhanced CDD measures in addition to the standard CDD measures when any of the following are identified as a PEP: a potential customer; an existing customer; the BO of a customer that is a legal person or other legal entity. The term *"politically exposed persons"* is defined in Art. 36(2) as a natural person who is, or who has been, entrusted with a prominent public function domestically, abroad or in an international organisation. The definition of prominent public functions is in line with the FATF standard.

(a) Art. 42(1) of the LMML requires OEs to establish effective internal systems for the purpose of determining whether a potential customer, existing customer or BO is a PEP. Art. 42(2) requires OEs to utilise at least one of the listed measures (sources of information) for determining whether a person is a PEP, which includes EDD measures, obtaining a written declaration from the customer on PEP status and/or relying on information obtained by using internal or external databases. Reliance on clients' declarations to reveal their PEP status, when it is used as the sole mean (i.e., without verifying information from reliable sources), would not fully amount to putting in place "risk management systems" to determine whether a customer or beneficial owner is a PEP, as prescribed by the FATF standard. Art. 25 of the RILMML only requires that more than one measure must be used where there is a higher risk.

(b) Art. 38 of the LMML requires senior management approval to commence or continue a business relationship with a customer or BO that is identified as a PEP.

(c) Art. 39 of the LMML requires OEs to take appropriate action to establish/clarify the source of funds and the source of wealth of the customer and any BO that is identified as a PEP.

Art. 27 of the RILMML requires comparison between information regarding source of wealth provided by the customer and of information obtained through CDD. The terms "source of funds" and "source of wealth" are not defined terms in law. However, guidance is provided by the ESA which is applicable to entities supervised by the BNB and other financial institutions. Also, a non-exhaustive list of examples is included in Appendix 4 of the RILMML.

(d) Art. 40 of the LMML requires OEs to conduct ongoing and enhanced monitoring of a business relationship with a customer or BO that is a PEP. Art. 37 extends the PEP requirement for at least 1 year after the prominent position is ceased and requires consideration of risks specific to the PEP before determining that measures are no longer required.

Criterion 12.2 – The definition of PEP does not distinguish between domestic and foreign PEPs. The enhanced measures set out under c.12.1 apply to all PEPs irrespective of whether they are domestic or foreign. Shortcomings related to internal controls applied to identify PEPs, as noted under c.12.1 apply here.

Criterion 12.3 – Art. 36 of the LMML extends the PEP definition to persons who are 'closely linked' with the customer or BO. 'Closely linked' is defined as including the following family members: spouses or persons in cohabitation, first-degree descendants and their spouses or persons in cohabitation; second-degree collateral relatives and their spouses or persons in cohabitation. It also includes persons in joint beneficial ownership or other close commercial, professional or other business relationship with the customer and a person who is BO of a legal person or other legal entity set up for the benefit of the customer or BO.

Criterion 12.4 – Art. 43 of the LMML requires insurers and insurance intermediaries to apply the internal processes for identifying whether a person is a PEP to policyholders and/or beneficiaries under life insurance contracts or other investment-related insurance contracts and/or the BOs of the policyholders, and/or the beneficiaries under such contracts.

Art. 43(2) of the LMML requires that articles 38 and 40 apply in cases where BOs or beneficiaries are identified as PEPs. Art. 38(1) and (2) of the LMML requires senior management approval to establish or continue a business relationship and Art. 40 of the LMML requires the OEs to conduct ongoing and enhanced monitoring of the relationship. Furthermore, Art. 43(3) of the LMML requires senior management to be notified of such a person being identified as a PEP prior to pay-out and requires the OE to consider making a disclosure to the FID-SANS, regardless of whether higher risks are present. Whilst there is a general requirement for ongoing and enhanced monitoring of a business relationship (Art. 40 of the LMML), there is no explicit requirement to conduct enhanced scrutiny on the whole business relationship with the policy holder before the pay-out when higher risks are identified.

Weighting and Conclusion

The following shortcomings apply: (i) OEs are permitted (except where higher risks are identified) to solely rely on clients' declarations to determine the PEP status (c.12.1. c.12.2). Considering the context of Bulgaria, namely, prevalent corruption, this is considered a severe shortcoming and thus weighted most heavily; (ii) There is no explicit requirement to conduct enhanced scrutiny on the whole business relationship with the policy holder before the pay-out when higher risks are identified (c.12.4).

Deficiencies relating to the financial services exempted from the regulatory environment are also relevant here.

R.12. is rated PC.

Recommendation 13 – Correspondent banking

In the 2013 MER, Bulgaria was rated LC with old R.7. Identified shortcomings were: (i) the requirement to gather sufficient information about the respondent institution was not extended to all FIs to cover relationships similar to correspondent banking relationships; (ii) the special measures applied only to non-EU correspondent relationships; and (iii) approval of an official at a senior managerial position before establishing a corresponding banking relationship was not required.

During the follow-up period Bulgaria took steps to address several deficiencies by introducing the relevant amendments to the provisions of the LMML. Nevertheless, moderate shortcomings remain as described below.

Criterion 13.1 – Art. 44(1) of the LMML requires OEs (including FIs), when establishing correspondent relationships that involve payments with third-country respondent institutions, to apply the following measures:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of the supervision, including whether it has been subject to ML/TF investigation or supervisory measures (regulatory actions)

(b) assess the respondent institution's AML/CFT controls

(c) obtain approval from senior management before establishing new correspondent relationships; and

(d) define and document the respective AML/CFT responsibilities of each institution. "*Third country*" is defined as a country which is not a Member State of the EU, therefore the LMML requirements do not apply to all cross-border relationships.

In accordance with Art. 74(a) of the LCI, banks are required to follow the European Supervisory Authorities Risk Factor Guidelines (ESA Guidelines)[109]. Section 8.10 of the ESA Guidelines prescribes that all correspondents should: (i) identify and verify the respondent institution and obtain sufficient information on respondent's business and reputation with a view to establishing that the ML risk of the respondent has not increased; (ii) consider, on a risk-sensitive basis, whether obtaining information about the respondent's major business, the types of customers it attracts, and the quality of its AML systems and controls (including publicly available information about any recent regulatory or criminal sanctions for AML failings) would be appropriate; (iii) establish and document responsibilities of each institution (respondent and correspondent); (iv) monitor the relationship and transactions; (v) ensure CDD is up to date, etc. However, these measures satisfy the requirements prescribed under c.13.1 only partly due to the following reasons: (a) no explicit reference is made to CFT; (b) obtaining information on the respondent's business, quality of the AML systems and controls and recent regulatory or criminal sanctions for AML failings is not strictly required in all cases; (c) no approval from senior management is required before establishing new correspondent relationships.

The full set of specific measures prescribed at c.13.1 is only required regarding correspondent relationships with a respondent institution from a non-EU/EEA Member State (see Art. 19 of the EU Directive 2015/849 and section 8.17 of the ESA Guidelines). The enhanced measures are required in circumstances where the risk associated with a respondent based in an EEA Member State is increased (see section 8.19 of the ESA Guidelines).

Criterion 13.2 – Art. 44 (2) of the LMML states that, where third parties who are customers of the respondent institution also have access to the payable-through account, OEs must be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to the accounts of the OE.

[109] Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849; EBA/GL/2021/02; March 1, 2021; https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors

Further, the LMML states that the OE must be satisfied that the respondent institution is able to provide relevant due diligence data immediately upon request.

Criterion 13.3 – Art. 45 (1) of the LMML prohibits OEs from establishing correspondent relationships with shell banks. In cases where a correspondent relationship with a shell bank has been established, the OE must immediately terminate such relationship. Art. 45(2) prohibits the OEs from establishing and maintaining correspondent relationship with an institution outside Bulgaria that allows its accounts to be used by shell banks.

There is no explicit requirement in the LMML to require FIs to satisfy themselves that a respondent FI does not permit its accounts to be used by shell banks. There is, however, such a requirement in the ESA Guidelines.

Weighting and Conclusion

The following shortcomings exist: (1) Measures described under c.13.1-2 are not applied to credit institutions within the EU/EEA within Bulgarian law, except for higher risk Member States through the implementation of EBA Guidelines (c.13.1); (2) There is no requirement for the FIs to satisfy themselves that the respondent FI does not permit its accounts to be used by shell banks other than in ESA Guidelines (c.13.3). **R. 13 is rated PC.**

Recommendation 14 – Money or value transfer services

In the 2013 MER, Bulgaria was rated C with old SR.VI.

Criterion 14.1 – The following types of *payment services* listed at Art. 4 of the LPSPS fall under the scope of MVTS: (i) placement of cash on a payment account and related services; (ii) services related to the operation of cash withdrawals; (iii) execution of payment transactions including transfers of funds on a payment account; (iv) execution of payments transactions where the funds are covered by a credit line; (v) issuing and or acquiring of payment instruments (which includes e-money issuers); (vi) money remittance. These services are provided by the electronic money institutions (EMI) and payment institutions (PI) that are OEs under Art. 4(2) of the LMML referred to as *other payment service providers.*

A separate category of OEs – postal money order (PMO) service providers – also offers money value transfer services (postal remittance). These persons are licensed by the CRC under Art. 39 of the Postal Services Act. The Postal Services Act does not provide for a definition of a "person" thus it is not clear as to whether natural persons can be authorised to provide postal money order services. Art. 39 of the Postal Services Act enables the CRC to grant an "individual licence" for the handling of postal money orders.

The LPSPS regulates the licensing of payment institutions (Art. 7) and the licensing of electronic money institutions (Art. 36(1))[110]. Foreign entities can operate under a home EU Member State licence (under free provision of services and right of establishment in the EU/EEA territory). For detailed information on EMI, PI, bank licensing requirements, please see R.26.

[110] Art. 7(1) of the LPSPS requires any person who intends to provide payment services to obtain a payment institution licence. A payment institution is required to be a legal entity. Art. 6 of the LPSPS states that the BNB shall issue a licence to conduct activity as a payment institution where the registered office of the applicant is in Bulgaria. Art. 36(2) of the LPSPS states that an electronic money institution licence is required prior to commencing issuing e-money. Art. 42 permits such entities to conduct other payment service activities.

Art. 2 of the LPSPS provides "negative scope" which removes various LPSPS requirements in certain cases, including paper-based vouchers and paper-based traveller's cheques which constitute "other stores of value". The disapplied requirements include licensing requirements under Chapter 2 of the LPSPS. Therefore, not all MVTS services envisaged by the FATF Standards are captured.

Criterion 14.2 – Art. 156 of the LPSPS empowers the BNB to investigate entities suspected of carrying out payment services without a licence, including powers to access premises and compel the production of information and records.

Art. 185(6) of the LPSPS states that a financial sanction shall be imposed for carrying out business without a licence ranging from BGN 5 000 (approx. €2 500) for a natural person to BGN 80 000 (approx. €40 000) for a legal entity in the event of recurrence provided that the act does not constitute an offence. In addition to the availability of administrative penalties under LPSPS, Art. 252 of the Criminal Code (Penal Code) provides two tiers of criminal penalties that are available where services are conducted without the proper licence. The lower tier penalty is a custodial sentence of three to five years and confiscation of up to ½ of the property of the perpetrator. The higher tier penalty is a custodial sentence of five to ten years, a fine of BGN 5 000 to BGN 10 000 (approx. €2 500 to 5 000) and court ordered property confiscation. The maximum penalty may be applied in cases where "consideration damages" have been caused or "considerable unlawful income has been obtained". Overall, considering the maximum amount of fines applicable and criminal penalties sanctions are proportionate and dissuasive in the context of Bulgaria.

In practice, the BNB identifies unlicensed MVTS providers through complaints received at the BNB, warnings received by Bulgarian competent and legal authorities or by competent authorities of another Member State as well as on the basis of information obtained by the BNB through checking publicly available information and the Commercial Register to flag entities that indicate MVTS (i.e., payment or e-money services) as their business activities.

Regarding the handling of postal money orders, the AT is advised that the CRC may investigate unlicensed persons on the basis of information provided through consumer complaints, whistle-blowers, competitors or competent authorities. Art. 99(1) of the Postal Services Act provides a penalty up to BGN 20 000 (approx. EUR 10 000) for a natural person and BGN 35 000 (approx. €17 500) for a legal entity or sole proprietor in respect of persons that continue to provide services in cases where the individual licence has been previously suspended or revoked. No offence is provided regarding services where no licence was previously held.

Criterion 14.3 – According to Art. 108 of the LMML and Art. 1a of the LMFT as well as Art. 32(e)(1) and Art. 32(e)(7)(18) of the RILSANS, the FID-SANS exercises control over the implementation of the LMML and LMFT, including the acts on their implementation by the PIs, EMIs and postal[111] money remittance service providers.

Art. 108 of the LMML and Art. 14a of the LMFT as well as Art. 79 of the LCI and Art. 154 (1), (2) and (6) of the LPSPS (regarding banks, payment institution and e-money institutions' supervision) permit the BNB, in its capacity as supervisor of credit institutions and other payment

[111]During the onsite the AT was advised that AML/CFT supervision of the postal money operators was conducted by the CRC as well as FID-SANS, however, no explicit legal basis has been established for CRC supervision of AML/CFT, as noted R.27.

service providers to exercise supervisory powers for AML/CFT purposes. For more information please also see R.26 and R.27.

Criterion 14.4 – Art. 32 of the LPSPS requires Bulgarian licensed institutions to notify the BNB of branches and agents. The BNB maintains a register of agents of payment service providers as required by Art. 19 (1)(1-2) of the LPSPS.

Art. 5 of the Postal Services Act permits the handling of postal money ordered by postal networks which includes "outreach postal offices" (i.e., agents) as defined at supplementary provision 1 (item 30) without any requirement for the agent to be licensed or registered or requirement for the CRC or PMO itself to maintain a current list of agents.

Criterion 14.5 – Art. 4(2) of the LMML applies requirements, including those regarding monitoring compliance, to payment service providers and their representatives (i.e., agents). Furthermore, Art. 101(8) specifically requires that the representatives comply with the OE's internal rules and Art. 65(2) of the RILMML requires the agent to provide the OE a declaration that they are familiar with the internal rules. However, there is no explicit requirement placed on the payment service provider to include their agents into the AML/CFT programmes and monitor for compliance with these programs.

Weighting and Conclusion

The following shortcomings exist: (i) paper-based vouchers and paper-based traveller's cheques which constitute "*other stores of value*" are exempted from the requirements (c.14.1); (ii) no sanctions available for persons carrying out postal money orders without a licence (this excludes persons and entities whose licence has been previously revoked or suspended) (c.14.2); (iii) there is no requirement for agents of PMOs to be licensed or registered by the CRC or the PMO itself to maintain a current list of agents (c.14.4); (iv) there are no explicit provisions to require inclusion of agents in AML/CFT programmes and monitoring (c.14.5). **R.14 is rated PC.**

Recommendation 15 – New technologies

In the 2013 MER, Bulgaria was rated compliant with former R. 8.

Criterion 15.1

Country level

At a national level, Art. 95(1) of the LMML provides a general requirement to conduct a national risk assessment of the ML/TF risks. Although there is no explicit legal requirement to assess risks related to development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products, Bulgaria has taken steps to analyse new technologies-related risks during its NRA exercise. It is covered under specific topics, rather than as a holistic risk assessment on the topic. For example, it is covered in Chapter 3: subsection drug trafficking and national vulnerabilities by new financial products; Chapter 5: ML risk assessment by economic sectors, subsection on IT and electronic money and Chapter 6: ML risk assessment in financial sector an DFNBPs sector, subsection e-money and virtual currencies.

Obliged entities level

Under Art. 48(2) of the LMML OEs are required to take appropriate actions to identify and assess the potential risks of money laundering or financing of terrorism arising from the introduction of new products, new business practices and new delivery mechanisms, as well as from the use of

new technologies for new or pre-existing products, business practices and delivery mechanisms. However, this requirement becomes mandatory when new products, business practices and delivery mechanisms are assessed as high risk in the NRA or in the business wide ML/TF risk assessment (BRA) performed by the OEs. Thus, implementation of the requirement is not explicit but rather a prerequisite (dependent on whether new technologies-related risks are identified as high in the NRA or BRA). Whilst Art. 30(1) of the RIMML notes that ML/TF risks associated with the new technologies must be assessed, it refers back to the process under Art. 48 (2) LMML.

This shortcoming, however, is partly mitigated by the requirements: (i) under articles 35(5) and 48(1- 3) of the LMML to apply enhanced CDD to the potential risks identified in the NRA arising from the introduction of new products, new business practices and new delivery mechanisms, as well as from the use of new technologies for new or pre-existing products, business practices and delivery mechanisms; and (ii) Art. 98 (1), (6) and Art. 99 (1) of the LMML to conduct risk assessments taking into account risk factors such as products, services and delivery channels.

Criterion 15.2

(a) Art. 48(3) of the LMML requires OEs to assess the risks before the introduction of new products, new business practices and new delivery mechanisms, as well as before the use of new technologies for new or pre-existing products, business practices and delivery mechanisms. However, the prerequisite for implementation of this requirement is when the new technologies-related risks assessed under NRA or BRA are high.

(b) Apart from general requirement to mitigate the risks, there is no explicit reference to take appropriate measures to manage and mitigate the risks that specifically target new and developing technologies, new business practices, new delivery mechanisms. However, this shortcoming is partly mitigated by the requirement under Art. 35(5) of the LMML, according to which OE have to take enhanced measures provided that new technologies-related risks are assessed as high as part of the NRA or BRA process or on the basis the results if the internal ML/TF risk assessment by the obliged entity. This is partly mitigated by Art. 30 (7) of the RILMML which states where a high risk of ML/TF is identified, enhanced CDD should be applied consistent with the risk.

Criterion 15.3

(a) An initial risk assessment of the virtual currency risk was carried out under the provisions of Art. 95 of the LMML that provides for national ML/TF risk assessment. The first NRA of Bulgaria was published January 2020 at http://www.dans.bg/en/msip-091209-menu-en/results-from-national-risk-assessment. It is covered under specific topics, rather than as a holistic risk assessment on the topic. For example, it is covered in Chapter 3: subsection drug trafficking and national vulnerabilities by new financial products - Chapter 5: ML risk assessment by economic sectors, subsection on IT and electronic money and Chapter 6: ML risk assessment in financial sector an DFNBPs sector, subsection e-money and virtual currencies. Bulgaria implemented the provisions relevant to VASPs included in 5AMLD, however, the definition under 5AMLD does not cover all VASP activities. According to the Art. 4(38) of the LMML, only the persons that by occupation provide exchange services between virtual currencies and recognised currencies that are not backed by gold are subject to AML/CFT regulation. The following VASPS services are not covered: (1) exchange between one or more forms of virtual assets; (2) transfer of virtual assets; (3) safekeeping and administration of virtual assets or instruments enabling control over virtual assets (4) participation and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The NRA assessed the risks with regard to virtual currencies as high both for ML and TF, although the assessment did not take in account the above mentioned VASPS as they do not fall under the scope of the AML/CFT regulation.

Whilst this initial risk assessment generally outlines some VASP activities, it does not currently cover the entire scope of the definition of VAs/VASPs covered by the FATF Recommendations. Both the Bulgarian authorities and FIs/DNFBPs are aware of the difference in the scope of virtual assets in the AMLD and FATF standard and Bulgaria note that changes to EU MIcA and the EU AMLD provisions are likely to align scope in the future. It is of note that Bulgaria has committed to conduct a VA sectorial risk assessment as one of the activities of the mentioned under c.1.3 in the future.

(b) Art. 96 and Art. 97 of LMML and Art. 59 of RILMML requires to assess and mitigate the risks identified in the NRA which includes virtual currencies to the extent they were covered. Bulgaria has not yet completed a developed risk treatment of the risks related to virtual currencies identified in the NRA and this is part of the Action Plan of the Intergovernmental working group under Art. 96 of LMML. The actions taken so far to manage and mitigate virtual assets related risks were not explicitly driven by the NRA results, but by the requirements of EU AML Directive. The actions taken so far encompass, e.g., including virtual currency exchangers and custodian wallet providers under the national AML/CFT regime (significant gaps relating to general coverage of virtual assets related activities apply here, see c. 15.3(a) for further information); introducing registration regime for virtual currency exchangers and custodian wallet providers.

(c) According to the Art. 4(38) of the LMML, only the persons that, by occupation provide exchange services between virtual currencies and recognised currencies that are not backed by gold are subject to AML/CFT regulation and thus are required to assess the risks in line with the requirements analysed under c.1.10 and c.1.11.

Criterion 15.4

(a) This criterion is addressed through Art. 9a of LMML and Ordinance № H-9 from 07.08.2020 issued by the Minister of Finance regarding the terms and procedure for entering in a register of persons that by occupation provide exchange services between virtual currencies and fiat currencies, and of custodian wallet providers (SG 72/14.08.2020). The VASPs registry is maintained by the National Revenue Agency.

The ordinance is in force since 19th August 2020 and respective entities were given 2 months term to register – i.e., by 19th October 2020.

(b) There are no legal provisions that would prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP.

Reference is made to c.15.3(a) related to limited coverage of VASPs-related activities in the country's legislation.

Criterion 15.5 – There are no legal or regulatory measures in place to identify unregistered VASPs and apply sanctions for provision of unlicensed (unregistered) services.

Criterion 15.6 – Providers of exchange services between fiat and virtual currencies are subject to AML/CFT measures in Bulgaria (Art. 4 (38) of he LMML). FID-SANS is the supervisory authority for VASPs, see more at R.27. However, supervision of this sector is not yet risk based.

Reference is made to c.15.3(a) related to limited coverage of VASPs-related activities in the country's legislation.

Criterion 15.7 – No specific AML/CFT guidelines and feedback have been issued for VASPs. The shortcomings identified under R.34 also apply here. Reference is made to c.15.3(a) related to limited coverage of VASPs-related activities in the country's legislation.

Criterion 15.8 – Shortcomings identified under R.35 apply here. Reference is made to c.15.3(a) related to limited coverage of VASPs-related activities in the country's legislation.

Criterion 15.9

(a) Although VASPs are considered OEs under the LMML Law, thus subject to the requirements analysed under the Recommendations 10 to 21, however, application of CDD is not triggered specifically under the circumstances referred to under sub-criterion 15.9(a), i.e., when the occasional transactions conducted by the VASPs equals or exceeds € 1 000.

As per Art. 11(1)(1-3) of the LMML, CDD requirements would be only triggered in the following circumstances: (1) when establishing business relationship; (2) when carrying out an occasional transaction amounting to or exceeding € 15 000 (incl. linked transactions); (3) when carrying out an occasional transaction amounting to or exceeding € 5 000 in cash (incl. linked transactions). These requirements are applicable to all OEs, thus equally applicable to VASPs.

(b) The EU Regulation (EU) 2015/847 which provide legal basis for compliance under the R.16 is not applicable to VASPs.

Criterion 15.10 – With respect to TFS, communication mechanisms explained under R.6 and R.7 apply to VASPs. Shortcomings identified at R.6 and 7 apply here, namely at sub-criterions c.6.6(g), c.7.2(e), c.7.4(d) and 7.3.

Criterion 15.11 – The analysis under R.37 – R.40 are also valid under this criterion, in relation to the FID-SANS powers to exchange information with foreign counterparts. Reference is made to c.15.3(a) related to limited coverage of VASPs-related activities in the country's legislation.

Weighting and Conclusion

The following shortcomings have been identified:(i) implementation of the requirement to assess the risk of new technologies is not explicit but rather a prerequisite (dependent on whether or not new technologies-related risks are identified as high in the NRA or business wide risk assessment); (ii) The following VASPS services are not covered: exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and administration of virtual assets or instruments enabling control over virtual assets participation and provision of financial services related to an issuer's offer and/or sale of a virtual asset; (iii) there are no legal provisions that would prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP; (iv) there are no legal or regulatory measures in place to identify unregistered VASPs and apply sanctions for provision of unlicensed services; (v) shortcomings identified under R.27, 34, 35, 37-40 apply to VASPs; (vi) VASPs are not required to conduct CDD when occasional transaction is equal or exceeds EUR 1 000 and no provisions exist requiring VASPs to comply with the elements of the R. 16; (vii) Shortcomings identified at R.6 and 7 equally apply to VASPs, namely at c.6.6(g), c.7.2(e), c.7.4(d) and 7.3. Consequently, **R.15 is rated PC.**

Recommendation 16 – Wire transfers

In the 2013 MER, Bulgaria was rated LC with old SR.VII, noting that the implementation and effectiveness of the EU Regulation could not be assessed.

Regulation (EU) 2015/847 is directly applicable for Bulgaria as of 26th of June, 2017. Reference to the Regulation is included in the LMML, LPSPS and BNB Ordinance No. 3.

For consistency reasons, the analysis below uses the terminology of the FATF Recommendations interchangeably with that of the Regulation (EU) 2015/847.

Criterion 16.1 – Art. 4(1-2) of Regulation (EU) 2015/847 implements the FATF requirement regarding all cross-border wire transfers of EUR 1 000 or more to always be accompanied by the required and accurate originator information, as well as by the required beneficiary information.

Further, Art. 11(4) of the LMML requires OEs to conduct CDD when carrying out an occasional operation or transaction which constitutes a transfer of funds as defined Art. 3 (item 9) of Regulation (EU) 2015/847, amounting to or exceeding EUR 1 000 or currency equivalent.

Criterion 16.2 – The FATF requirements regarding batch files are implemented through Art. 6 of Regulation (EU) 2015/847 with relevant references to Art. 6, 7(2) and 11(2)(c) for required and accurate originator information, as well as for required beneficiary information, including the originator's payment account number or unique transaction identifier, that is fully traceable**.**

Criterion 16.3 – According to Art. 6 of Regulation (EU) 2015/847, cross-border wire transfers below EUR 1 000 are required to be accompanied by the originator and beneficiary information.

Criterion 16.4 – According to Art. 6 of Regulation (EU) 2015/847, FIs need not verify the information on the originator unless, inter alia, they have reasonable grounds for suspecting ML/TF.

Criterion 16.5 and 16.6 – Wire transfers within the EEA are considered domestic transfers for the purposes of R.16, which is consistent with the FATF Standards.

Art. 5 of Regulation (EU) 2015/847 defines that such transfers shall be accompanied by at least the payment account number of both the originator and the beneficiary, or by the unique transaction identifier. At that, there is a three working day period established for the ordering FI to make available required originator information whenever requested to do so by the beneficiary or intermediary FI. Art. 14 of the Regulation requires FIs to respond fully and without delay to enquiries from appropriate AML/CFT authorities.

Criterion 16.7 – Art. 16 of Regulation (EU) 2015/847 establishes a five-year period for ordering and beneficiary FIs to retain the records of originator and beneficiary information. The Regulation defines that Member States may allow or require further retention only after they have carried out a thorough assessment of the necessity and proportionality of such further retention, and where they consider it to be justified as necessary for the ML/TF purposes. That further retention period shall not exceed five years.

Criterion 16.8 – Art. 4 of Regulation (EU) 2015/847 prohibits the ordering FI from executing any transfer of funds before ensuring full compliance with its obligations concerning the information accompanying transfers of funds.

Criterion 16.9 – Art. 10 of Regulation (EU) 2015/847 requires intermediary FIs to ensure that all the information received on the originator and the beneficiary, that accompanies a transfer of funds, is retained with the transfer.

Criterion 16.10 – Regulation (EU) 2015/847 does not provide for the exemption specified in this criterion regarding technical limitations preventing appropriate implementation of the requirements on domestic wire transfers.

Criterion 16.11 – Art. 11 of Regulation (EU) 2015/847 stipulates the obligation of the intermediary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or required beneficiary information in a transfer of funds is missing.

Criterion 16.12 – Art. 12 of Regulation (EU) 2015/847 stipulates the obligation of the intermediary FI to establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required originator and required beneficiary information and for taking the appropriate follow-up action.

Criterion 16.13 – Art. 7 of Regulation (EU) 2015/847 stipulates the obligation of the beneficiary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or required beneficiary information in a transfer of funds is missing.

Criterion 16.14 – Art. 7 of Regulation (EU) 2015/ 847 defines that, in the case of transfers of funds exceeding EUR 1 000, the beneficiary FI shall verify the accuracy of the identification information on the beneficiaries before crediting their payment account or making the funds available to them. Art. 16 of Regulation (EU) 2015/847 requires ordering and beneficiary payment service providers to keep this information for 5 years.

Criterion 16.15 – Art. 8 of Regulation (EU) 2015/847 stipulates the obligation of the beneficiary FI to implement effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required originator and beneficiary information and for taking the appropriate follow-up action.

Criterion 16.16 – The Regulation (EU) 2015/847 is binding for all MVTS providers, including their agents (Art. 2(1)).

As established at c.14.1 paper-based vouchers and paper-based traveller's cheques which constitute "other stores of value" are not included in the scope of MVTS.

Criterion 16.17 – Articles 9 and 13 of the Regulation (EU) 2015/847 require beneficiary and intermediary FIs to take into account missing or incomplete information on the originator or the beneficiary as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported. Art. 4 of the Regulation, in turn, prohibits ordering FIs from executing any transfer of funds before ensuring full compliance with the obligations on accompanying information. Overall, there is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer, in cases where a MVTS provider controls both the sending and receiving end of the transfer.

Criterion 16.18 – FIs conducting wire transfers are subject to the EU Regulations and domestic measures taken according to UNSCRs 1267, 1373 and their successors.

Weighting and Conclusion

Bulgaria complies with most of the requirements under R.16. However, some deficiencies exist: (i) paper-based vouchers and paper-based traveller's cheques which constitute "*other stores of value*" are not included in scope of MVTS (c.16.16); (ii) there is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer,

in cases where an MVTS provider controls both the sending and receiving end of the transfer (c.16.17). **R. 16 is rated LC.**

Recommendation 17 – Reliance on third parties

In the 2013 MER, Bulgaria was rated compliant with former R. 9.

Criterion 17.1 – Only certain FIs are permitted to rely on third parties regarding certain elements of CDD. Bulgarian authorities advise that permitted entity types were determined on the basis of risk, including by assessing the effectiveness of AML/CFT preventatives measures applied by different categories of the OEs.

Art. 56(1) of the LMML stipulates conditions for core principles FIs (currency exchanges offices, leasing undertakings, postal operators and all DNFBPs are excluded) to rely on a prior identification of a customer by a credit institution to obtain CDD data, namely identification and verification of the customer and beneficial owner (purpose and nature of business relationship does not form an integral part of CDD which is relied upon). Art. 56(3) states that such reliance shall not release the OE of liability for failure to apply CDD measures. Reliance is permitted only where the following conditions are met:

(a) according to Art. 56(1)(2) of the LMML CDD information referred above must be made available immediately upon request from a third-party

(b) Art. 56(1)(2-3) of the LMML requires the credit institutions to provide information and copies of documents to the requesting OE immediately upon request, whereas certified copies of relevant documents shall be submitted to the OE within 3 days.

(c) there is no explicit requirement for the OE to satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11. However, the limitations on use at Art. 56(1)(3) effectively require consideration of whether requirements for regulation, supervision and monitoring are satisfactory thereby meeting the requirements of 17.1(c).

Criterion 17.2 – Art. 56(1)(1) of the LMML requires the OE to consider the level of country risk of the credit institution upon which reliance can be placed. In addition, Art. 56(3)(2) specifically prohibits reliance on third parties located in a high-risk country.

Criterion 17.3 – Art. 57(1) of the LMML permits all OEs to rely on another entity within the same group regarding identification and verification of the customer and beneficial owner, provided that the below conditions are met.

(a) The group applies CDD, record-keeping and programmes against ML and TF in accordance with LMML (Art. 57(1)(2) of the LMML).

(b) The effective implementation of CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority (Art. 57(1)(3) of the LMML).

(c) OEs that are part of a group are required to implement group-wide procedures and such procedures must be commensurate with the nature and size of the OE's business and effectively manage and mitigate ML/TF risks (Art. 104(1) of the LMML).

Weighting and Conclusion

R. 17 is rated C.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 2013 MER, the Republic of Bulgaria was rated LC with former R.15. The assessment identified technical deficiencies related to employee screening, audit controls and testing, and the application of internal programmes.

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 18.1 – Art. 101 of the LMML requires OEs to adopt internal rules and controls in accordance with the terms and procedure set out in the RILMML, which must be risk-based and proportionate to the size of the OE. Such rules and controls must be applied effectively by branches and subsidiaries.

(a) Compliance management arrangements

In the LMML, two types of arrangement are permitted; "*specialised service*" (which effectively constitutes an AML/CFT Unit within the OE) or designation of a single responsible person.

Art. 106(1) of the LMML requires all core principle FIs to establish a specialised service whereas Art. 107(2) of the LMML permits all other OEs to designate a single responsible person in cases where no specialised service has been established. Art. 106(2) of the LMML states that the specialised service shall be headed by a senior management employee who is responsible for the implementation of internal controls.

Art. 107(3) of the LMML states that a senior management employee may, by written instrument, be designated to implement internal controls. In both cases, there is a requirement to notify FID-SANS of the responsible persons (Articles 106(5) and 107(4) of the LMML).

(b) *Employee* screening

There is no requirement in the LMML for OEs to have internal screening procedures to ensure high standards when hiring employees. Although, the LCI, BNB Ordinance 20, IC, MFIA and CISCOUA do include certain integrity and competence requirements for some employees in the banking and securities industry, this does not satisfy the requirement to have screening procedures (internal policies and controls) in place.

(c) Ongoing training

Art. 101(2)(13-14) of the LMML requires OEs to establish rules for employees training. In addition, under Art. 101(4)(11) of the LMML OEs are required to provide initial and continuing training to employees to make employees aware of the provisions of the AML/CFT requirements, OE's internal rules and controls, including the handling of suspicion of ML/TF.

(d) Independent audit function

Art. 101(2)(3-4) of the LMML requires the OEs to establish rules containing the "*possibility of carrying out an internal audit review*" and "*possibility of conducting an independent audit to test and evaluate compliance, where appropriate with regard to the size and nature of the business*". It does not seem, however, that the requirement for an audit is mandatory due to the following reasons: (i) the legislation uses wording "possibility" rather than require an audit; (ii) possibility for an audit is dependent on the size and nature of business.

In the case of banks, internal audit is mandatory under the BNB Ordinance 10. Art. 8(1) item 4 of the BNB Ordinance 10 establishes the requirement for internal audit, Art.16(1) of the BNB Ordinance 10 requires independence and Articles16(3) and Art. 17 of the BNB Ordinance 10 establish the scope of the audit. However, there is no explicit reference to the AML/CFT audit. Also, Section 22 of the EBA Guidelines of Internal Governance 2017 which are legally enforceable under Art. 74(a) of the LCI requires to set up independent and effective internal audit functions. However, neither BNB Ordinance 10, nor EBA Guidelines of Internal Governance do not explicitly refer to AML/CFT audit.

Criterion 18.2 – Art. 104(1) of the LMML requires OEs that are part of a group to adopt group-wide procedures that include the AML/CFT requirements referred to under c.18.1 or comply with the said requirements by other means. "*Other means*" prescribes that having group-wide policies and procedures is not obligatory in all cases. Shortcomings identified under c.18.1 apply here.

Paragraph 1(2) of the LMML defines "*Group*" as a parent undertaking, its subsidiaries, and the legal entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other.

(a) Information sharing

Art. 101(2)(10) of the LMML requires OEs to establish terms and procedures for the collection, retention and disclosure of information. All of these requirements apply to branches and subsidiaries located abroad.

(b) Provision of AML/CFT information by group-level functions

Art. 80(3) permits disclosure of AML/CFT related data and information only for payment service providers, credit institutions and entities operating in insurance and securities market that are part of the same group. Other FIs, such as leasing undertakings and postal operators are excluded.

Art. 72(6-7) of the LMML requires that information regarding suspicious activity reports filed to FID-SANS be shared within the group except where FID-SANS instructs otherwise. However, there is no explicit requirement to share information regarding unusual activity and/or its analysis.

(c) Safeguards

Art. 83 of the LMML states that personal data shared under the LMML shall not be processed other than for AML/CFT purposes. Art. 80(1) of the LMML prohibits OEs from notifying the customer or third parties regarding disclosures of information. Whilst there is no explicit reference that group-wide programmes against ML/TF should contain adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off, Art. 104 of the LMML requires group-wide policies and procedures to be applied to all members of the group: the terms for the collection, retention and disclosure of information constitutes part of these group wide procedures.

Criterion 18.3 – Art. 7(1-2) of the LMML requires OEs to ensure the effective application of measures by branches and subsidiaries in third countries, including the sharing of information, in so far as is permitted under the legislation of the third country. Where the legislation of a third country does not permit or restricts the application of the measures under the LMML and RILMML, the OEs are required, at Art. 7(2) of the LMML, to notify the FID-SANS and the relevant supervisory authority and to take additional measures in accordance with the risks. However,

the requirements under Art. 7(1-2) of the LMML are not applicable to foreign branches and majority owned subsidiaries located in the EU countries.

The RILMML prescribes additional safeguards relevant for proper risk management purposes: (i) Art. 1 of the RILMML requires OEs to risk assess foreign branches and subsidiaries and factor such considerations into senior management approved procedures and training; (ii) Articles 3 - 15 of the RILMML provide additional measures that shall be applied in cases where the legislation of the host country does not permit or limits the effectiveness of measures, including the requirement to inform FID-SANS. The legislation does not explicitly cover a scenario where AML/CFT requirements of the host country are less strict than those of the home country.

Weighting and Conclusion

Following shortcomings exist: (i) no requirement to have policies and procedures on employee screening to ensure high standards when hiring (c.18.1(b)); (ii) internal AML/CFT audit function is not mandatory (c.18.1(d)); (iii) compliance with AML/CFT requirements via group-wide procedures is not mandatory, "*other means*" are permitted (c.18.2); (iv) disclosure of AML/CFT related data and information is permitted only for payment service providers, credit institutions and entities operating in insurance and securities market and does not cover other FIs (c.18.2(b)); (v) there is no explicit requirement to share information regarding unusual activity and/or its analysis between group entities (c.18.2(b)); (vi) disclosure of information within a group is permitted only for certain types of FI (c.18.2(b)); (vii) there are no requirements to have group wide programmes on adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off (c.18.3); (viii) Requirement to ensure that foreign branches and subsidiaries apply AML/CFT measures consistent with the home country requirements do not extend to EU countries; (ix) the legislation does not explicitly cover a scenario where AML/CFT requirements of the host country are less strict than those of the home country. Deficiencies relating to the services exempted from the regulatory environment also apply here.

Consequently, **R. 18 is rated PC.**

Recommendation 19 – Higher-risk countries

In the 2013 MER, Bulgaria was rated LC with old R.21. The deficiency identified related to effectiveness: the FIs were not fully clear what countermeasures were applicable in the cases of countries that do not, or not fully apply, the FATF Recommendations.

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 19.1 – Art. 35 item 2 of the LMML requires OEs to apply enhanced CDD measures when entering into a business relationship and in the course of any such relationship as well as when carrying out an occasional operation or transaction with natural persons, legal persons and arrangements from a high-risk third country.

Art. 46(3) of the LMML states that high-risk third countries are those which do not apply, or apply incompletely, the international standards for AML/CFT as identified by the EC. Further, it states that lists of such countries shall be published on the websites of the FID-SANS, BNB, FSC, NaRA and MoF. Art. 46(5) of the LMML permits the FID-SANS to instruct application of enhanced CDD

measures in cases of business relationships and/or occasional transactions with natural and legal persons and other legal entities from countries which are not included in the list of the EC. Although the EC Lists published on the website of FID-SANS, and the FSC are broadly aligned with the FATF lists, the legislation does not provide any explicit reference to the high risk third countries identified by the FATF.

Although Art. 51(1)(2) of the LMML requires, when deciding upon enhanced CDD measures with a view to mitigating the risks, to "take account of" measures considered appropriate by the FATF and Art. 16(3) of the RILMML states that OEs "may" take into consideration FATF guidance and decisions, it is not explicit that FIs must apply enhanced CDD in accordance with FATF publications on high-risk countries.

In addition, there is no explicit requirement that EDD measures applied to clients from high risk third countries should be proportionate to the risks, however, there exists an overarching requirement at Art. 98(9) and 51(1) to apply all LMML measures on the basis of conducted risk assessments by the OEs.

Criterion 19.2 – Art. 46(3) of the LMML states that FID-SANS shall maintain a list of countries identified by the EC as high risk on its website and Art. 46(5) permits FID-SANS to require application of enhanced CDD measures to persons of countries outside of the list referred to in Art. 46(3).

In addition, Art. 46a(4) of the LMML empowers the FID-SANS or the relevant supervisory authority to apply countermeasures in higher risk situations.

Whilst the additional measures required at Art. 46a(4) are consistent with the countermeasures envisaged by the FATF Recommendations, the identification of high-risk countries does not fully constitute jurisdictions subject to a FATF call for countermeasures.

Criterion 19.3 – As stated under c.19.1, the LMML requires high-risk country lists to be published on the websites of the FID-SANS, BNB, FSC, NaRA and MoF. The published lists are broadly aligned with the FATF lists, as discussed at c.19.1.

Weighting and Conclusion

The following shortcomings exist: (1) no explicit reference to high risk third countries identified by the FATF, including the "*counter measures list*"; (2) no explicit requirement for enhanced CDD to be proportionate to the risks; (3) published high-risk country lists are not entirely aligned with the FATF lists. Deficiencies relating to the services exempted from the regulatory environment also apply here. **R.19 is rated LC.**

Recommendation 20 – Reporting of suspicious transaction

In the 2013 MER, Bulgaria was rated LC with old R.13. The assessment identified technical deficiencies related to the criminalisation of ML and a restriction in reporting scope.

Deficiencies relating to the financial services exempted from the regulatory environment apply here i.e., licensing and supervisory regime does not cover safekeeping services and payment services related to paper-based vouchers and paper-based traveller's cheques (except where carried out by a bank). See R.26 for more information.

Criterion 20.1 – Art. 72(1) of the LMML requires OEs to report immediately to FID-SANS whenever there is suspicion or knowledge of ML or that "*proceeds of criminal activity are involved*" before carrying out a transaction or operation. Criminal activity means all crimes under the Penal

(Criminal) Code. In cases where delay is "likely to frustrate the action for persecution of beneficiaries", the report may be made immediately following the transaction.

Regarding TF, there are two types of disclosure. Art. 9(3) of the LMFT requires OEs to report knowledge or suspicion of TF immediately to the FID-SANS before the operation or transaction is carried out and to delay the execution of said operation or transaction within the time allowed. In addition, Art. 9(1) provides an additional requirement for any person, who *knows* that given financial operations or transactions are intended to finance terrorism, to notify immediately the Minister of Interior and the Chairperson of the State Agency for National Security.

Neither the LMML, nor LMFT explicitly cover circumstances where there are reasonable grounds to suspect.

Criterion 20.2 – Articles 72(5) of the LMML and 9(4) of the LMFT specifically require reports to be made in relation to attempted transactions provided that they are suspicious. Neither provide for any de minimis threshold.

Weighting and Conclusion

There is no explicit requirement to report in cases where there are *reasonable grounds* to suspect ML/TF. Deficiencies relating to the services exempted from the regulatory environment also apply here. **R. 20 is rated LC.**

Recommendation 21 – Tipping-off and confidentiality

In the 2013 MER, Bulgaria was rated LC with former R.14. The assessment identified technical deficiencies related to protection from civil liability.

Criterion 21.1 – Art. 86(1) of the LMML provides that ML disclosures made under the provisions of the LMML shall not give rise to liability for a breach of any restriction on disclosure of information. This extends to all employees under Art. 72(3) of the LMML. Further, Art. 86(2) of the LMML extends such protections in cases where it is established that not criminal offence has been committed. Similar provisions regarding TF disclosures are included within Articles 9(10), (6) and (11) of the LMFT.

Criterion 21.2 – Art. 80(1) of the LMML prohibits OEs including the persons who manage and represent the entity and employees from notifying the customer or third parties of the disclosure of information. Articles 80 (3), 72 (6) and 72 (7) of the LMML provide an exemption to this prohibition regarding information sharing within a group. Similar provisions regarding TF disclosures are included within Articles 9(13), (14) and (15) of the LMFT. The following shortcomings identified at R.18 are relevant here: (i) there are no explicit legal requirements relating to safeguards on the confidentiality and information exchanged, specifically referred to the safeguards of tipping off prevention; (ii) limitations apply concerning information sharing between group entities relating to unusual activities. See R.18 for more information.

Weighting and Conclusion

Minor shortcomings identified at R.18 apply here: (i) there are no explicit legal requirements relating to safeguards on the confidentiality of information exchanged, specifically regarding safeguards of tipping off prevention; (ii) limitations apply concerning information sharing between group entities relating to unusual activities. **R. 21 is rated LC.**

Recommendation 22 – DNFBPs: Customer due diligence

In the 2013 MER, Bulgaria was rated PC with the old R.12. The assessment identified technical deficiencies related to those identified under old R.5.

In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

Criterion 22.1 CDD measures apply to all "*obliged entities*" as listed in Art. 4 of the LMML be they FIs or DNFBPs. The activities listed are broadly equivalent to those envisaged by the Standard. Where no specific provisions exist regarding when CDD is to be carried out by a particular OE, the general requirement at Art. 11 of the LMML applies (see c.10.2).

(a) Casinos

Listed at item 21 of Art. 4 of the LMML are the organisers of gambling games, licenced to organise gambling games within the territory of the Republic of Bulgaria pursuant to the Gambling Act. Art 12 of the LMML requires gambling operators to apply CDD measures where the wagering of stakes, payment of winnings or the purchase or exchange of chips equal or exceed EUR 2 000 or currency equivalent are carried out in a single operation or in several linked operations.

(b) Real estate agents

Listed at Art. 4(18) of the LMML are persons providing by occupation intermediation in real estate transactions, including with respect to real estate rental transactions where the monthly rent amounts to or exceeds EUR 10 000 or currency equivalent.

(c) Dealers in precious metals and stones

The FATF requirement to apply measures to dealers in precious metals and stones applies only in cases where they engage in a cash transaction with a customer equal to or exceeding EUR 15 000. Since 2012, the LCPA has prohibited the use of cash for transactions equal to or exceeding BGN 10 000 except in limited scenarios. As such, the list of OEs at Art.4 of the LMML does not include dealers in precious metals and stones.

(d) Lawyers, notaries, other independent legal professional and accountants

Listed at item 15 of Art. 4of the LMML are persons that, by way of business, provide legal advice regarding wide range of services, including where they act for or on behalf of a customer, provide a registered office or correspondence address or other related services or assist or participate in operators and transactions, concerning -

- buying and selling of immovable property;
- managing funds, financial instruments or other assets;
- opening, managing or disposing of a bank account, savings account or financial instruments account;
- organising contributions necessary for the creation or operation of legal person or other legal entity;
- formation, registration, organisation of the operation or management of a trust, merchant or another legal person, or other legal entity; and
- fiduciary management of property.

(e) *Trust and company service providers.*

Listed at item 16 of Art. 4of the LMML are persons that, by way of business, provide:

- a registered office, correspondence address, business accommodation and/or other related services for the purposes of the registration and/or operation of a legal person or other legal entity;
- services comprising the formation, registration, organisation of the operation and/or management of a merchant or of another legal person, or other legal entity;
- services comprising the fiduciary management of property;
- acting as, or arranging for another person to act as, a director, a secretary, a partner or a similar position in a legal person or other legal entity;
- acting as, or arranging for another person to act as, a trustee, in cases of trusts, escrow funds and other similar foreign legal arrangements incorporated and existing under the law of the jurisdictions providing for such forms of trusts (trusts cannot be established under Bulgarian law);
- acting as, or arranging for another person to act as, a nominee shareholder in a third-party foreign legal person or legal entity other than a company listed on a regulated market that is subject to disclosure requirements in accordance with European Union law or subject to equivalent international standards.

The deficiencies identified under R.10 also apply to DNFBPs.

Criterion 22.2 – Reference is made to the analysis for R.11 on the general coverage of recordkeeping requirements within Bulgarian legislation, which are equally applicable to DNFBPs.

Criterion 22.3 – Reference is made to the analysis for R.12 on the general coverage of PEP requirements within Bulgarian legislation, which are equally applicable to DNFBPs.

Criterion 22.4 – Reference is made to the analysis for R.15, which is equally applicable to DNFBPs.

Criterion 22.5 – Reference is made to the analysis for R.17 on the reliance provisions, part of which is applicable to DNFBPs.

Weighting and Conclusion

Based on deficiencies identified in R.10 (PC), 11 (LC) 12 (PC), 15 (PC) and 17 (C) which are relevant to DNFBPs, **R. 22 is rated PC.**

Recommendation 23 – DNFBPs: Other measures

In the 2013 MER, Bulgaria was rated LC with old R.16. The assessment identified technical deficiencies related to those identified for FIs.

In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

Criterion 23.1 – Reference is made to the analysis for R.20 on the general coverage of STR requirements within Bulgarian legislation.

Criterion 23.2 – Reference is made to the analysis for R.18 on the general coverage of internal control requirements within Bulgarian legislation. In addition, disclosure of AML/CFT related data and information is not permitted for DNFBP groups (c.18.2(c)).

Criterion 23.3 – Reference is made to the analysis for R.19 on the general coverage of the requirements regarding high-risk countries within Bulgarian legislation.

Criterion 23.4 – Reference is made to the analysis for R.21 on the general coverage of the tipping-off and confidentiality requirements within Bulgarian legislation.

Weighting and Conclusion

Based on deficiencies identified in Recommendations 18(PC), 19(LC), 20(LC), 21(LC) which are relevant to DNFBPs. **R. 23 is rated LC.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

In the 2013 MER, Bulgaria was rated largely compliant with former R. 33 due to the shortcomings relating to the ownership of the bearer shares that is not verifiable at the Commercial Register or any other register.

Criterion 24.1 – Bulgaria describes the types, forms and basic features of legal persons in a variety of different pieces of legislation. The vast majority of legal forms in Bulgaria are Companies (Commerce Act (CA)), Non-Profit Legal Entities (Non-Profit Legal Entities Act (NPLEA)), Cooperatives (Cooperatives Act (CoopA). Other legal forms include: (1) legal persons established under the National Community Centers Act or specialized national administrations and agencies established by a special normative deed (e.g. The National Agency for the State reserve and war time supplies established under the State Reserve and War time Supplies Act); (2) Certain other legal entities (which are established as JSCs or LLCs) which carry out a national function or are owned (in majority or in full) by the State are established by special legal acts (such as the Medical Establishments Act, the Public Enterprises Act, etc.) and these acts provide additional requirements as to their establishment, existence, directors, etc.

The types of companies referred to under Art. 64(1) of the CA are the following: 1. general partnership; 2. limited partnership; 3. limited liability company; 4. joint stock company; 5. limited stock partnership.

The process for the incorporation of each type of legal person/entity is described in the respective legal act. Additionally, the necessary documentation for their entering in the CRNPLER are listed in detail in Ordinance No 1 from 14.02.2007 for Keeping, Storage and Access to the Commercial Register and to the Register of Non-Profit Legal Entities (OKSACRRNPLE).

Although the processes of incorporation vary depending on the different types of legal persons/entities, there are similarities. For example, the establishers of all of the legal persons obliged by the law to enter in the Commercial Register and the Non-Profit Legal Entities Register (CRNPLER) (except for the Sole entrepreneurs) are required to convene and hold a constituent assembly the purpose of which is to establish the name, location, activity, managing body/managing bodies, type of management, capital etc. The resolutions adopted in the constituent assembly are incorporated within a Memorandum/Constitutive deed/By-Laws/Articles of Association depending on the type of legal person, and it is submitted in the electronic lot of the legal person and is freely available for review and download.

Upon registration within the Commercial Register and the Non-Profit Entities Register (CRNPLER) each legal person/entity receives randomly generated nine-digit unified identification code (UIC) as well as an electronic lot.

The CRNPLER holds the electronic lots of the legal persons/entities. Each electronic contains information on a variety of areas:

- **General Information -** It contains information regarding but not limited to the name, the type of legal person/entity, detailed information regarding the headquarters and address of management, the activity of the company, the representatives and the method of representation /if applicable/, the term of existence /if applicable/, the special conditions /if applicable/, the amount of the capital /if applicable/ in Bulgarian Levs as well as detailed description of the non-monetary contribution /if applicable/, its monetary value, and the grounds of the contributor's rights, names of the persons as well as name and identification number for legal person/entity, partners, respectively sole owners /if applicable/etc.
- **Liquidation** /which includes the names of the liquidator as well as the term of liquidation etc.
- **Bankruptcy and Resolutions from court proceedings regarding Bankruptcy** /containing information regarding the bankruptcy procedures such as date of insolvency, bankruptcy administrator, all of the resolutions of the court regarding the bankruptcy proceedings for the respective legal person/entity etc.
- **Preservation orders on the company shares** /information regarding the debtor, the amount of the obligation, information regarding the public enforcer managing the case etc.
- **Pledges** /over all or part of the shares or over the legal person entity/entity as a whole containing information regarding the pledge contract, its parties, the pledge creditor etc.
- **Beneficial owners** - containing information of the beneficial owners of the company.

Information in the different sections is publicly available. Archived information is available to registered individuals.

The provision for recording basic information for the legal entities provided for in the CA and for their entry in the Commercial Register is found in Art. 78; Art. 79(2); Art. 102, Art. 103; Art. 113, Art. 115; Art. 119; Art. 129; Art. 140; Art. 163; Art. 174; Art. 192a; Art. 253 of the CA.

The provision for recording basic information for non-profit legal entities as well as for their entry in the Register of non-profit legal entities and for changes in circumstances is found in Art. 17–20; Art. 33–36; Art. 39; Art. 44a–44в of the NPLEA.

The provision for recording basic information in respect of Cooperatives is contained in the CoopA – Art. 1-2.

There is also more detailed information available in Bulgarian on the website concerning the registration process on each individual application, which includes specific information on document submission and information on processing applications. This information includes requirements, procedures, instructions, application samples, relevant legislation and payment methods.

Criterion 24.2 – Currently, the risk assessment of ML risks associated with all types of legal persons created in the Bulgaria conducted through the NRA exercise is high level and whilst it focusses on some risks associated with certain types of legal persons (LLCs) - notably in Chapter 4, it does not represent a comprehensive systematic risk assessment of the risks associated with all types of legal persons in Bulgaria. The analysis of the inherent vulnerabilities of each relevant type of legal entity is currently not complete and the current analysis is very much driven by recent operational activity and does not adequately cover all entities and their exposure to risk in Bulgaria.

Criterion 24.3 – All legal entities, branches of foreign legal entities, NPOs and branches of foreign NPOs shall be entered in the Commercial register and Non-profit legal entities register (CRNPLER) held by the Registry Agency (Art. 2(1) of the ACRNPLER). The basic information which shall be entered in the registers depends on the type of the legal entity or arrangement and is described in the respective laws and in the Ordinance No 1 from 14.02.2007 for Keeping, Storage and Access to the Commercial Register and to the Register of Non-Profit Legal Entities (OKSACRRNPLE). Basic information commonly includes company name, legal form, the address of the registered office, a list of directors or managers, capital, memorandum of association, incorporation, the statues, etc. This information is publicly available.

Criterion 24.4 – All legal entities are required to record protocols and other documentation regarding their incorporation and any change to information that occurs after this time. The legal entities are required by law to submit the relevant documentation for incorporation or changes within 7-days term (Art. 6(2) of the ACRNPLER) or other term if such is explicitly determined in a specific law (for example longer term for the entry is provided in Art. 18(5) of the NPLEA). The requirements are contained in the Companies (Commerce Act (CA)), Non-Profit Legal Entities (Non-Profit Legal Entities Act (NPLEA)), Cooperatives (Cooperatives Act (CoopA), Community Culture Centres (the National Community Centers Act). There are also relevant provisions directly applicable under Regulation (EEC) No 2137/85, Regulation (EC) No 1435/2003, Regulation (EEC) No 2157/2001.

Art. 179 of the CA contains requirements for Companies to keep a register of their shareholders in which the names and addresses, the Single Identity Number/Personal Identification Number or Uniform Identification Code of the holders of registered stocks shall be recorded along with the type, nominal value and issue price, quantity and serial numbers of the stocks shall be indicated. This requirement also applies to interim certificates. The person, or persons, representing the company, shall be obliged to ensure the entry into the register of this information and changes within 7 days,

However, there are no specific provisions in Bulgaria to ensure that basic information is always maintained within the country at a location notified to the companies' registry.

Criterion 24.5 – In case of any change in the basic information in the registers, an application for entering of the changes is to be submitted within 7 days, pursuant to the general provision of Art. 6(2) of the ACRNPLER and Art. 12(4) of the BRA. Art. 179 of the CA also contains requirements that shareholder information is updated within 7 days of submission to the person or persons representing the company.

However, there are not sufficient mechanisms in Bulgaria to ensure accuracy of the basic information. Art. 13(4) of the ACRRNPOs and the provision of Art. 313 of the Penal Code make the declaring of untrue information a crime but no further provisions as to accuracy exist.

No additional information has been provided by the Bulgarian authorities concerning the cases where information is not entered in the Registry (due to the fact that entities are not subject to registration) and has to be maintained by the legal person.

Criterion 24.6

(a) Art. 61(1) of the LMML covers the obligation of all legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria and the natural contact persons to obtain, hold and provide adequate, accurate and current information on the natural persons who are the beneficial owners thereof, including the details of the beneficial interests held by the said natural persons.

Beneficial Owner is defined in § 2 of the Supplementary Provisions to the LMML and covers any natural person or persons who ultimately owns or controls a legal person or other legal entity, and/or any natural person or natural persons on whose behalf and/or for whose account an operation, transaction or activity is being conducted. It applies if either they hold a sufficient percentage of the shares, ownership interest or voting rights in that legal person or if they hold a shareholding or an ownership interest of at least 25 per cent in a legal person or other legal entity held by a natural person or persons (by way of indirect ownership) or a shareholding or an ownership interest of at least 25 per cent in a legal person or other legal entity held by a legal person or other legal entity which is under the control of one and the same natural person or natural persons or by multiple legal persons and/or legal entities which are ultimately under the control of one and the same natural person/persons, shall be an indication of indirect ownership.

The inclusion of the terminology sufficient percentage of the shares is unclear in its operation when compared to the 25 per cent requirement described.

Minor shortcomings identified at c.10.10 apply here: the LMML does not explicitly state that an OE must identify and take reasonable measure to verify the identity of a natural person who exercises control through other means than ownership in the circumstances included within c.10.1, where (a) there is doubt that a person with the controlling ownership interest is a beneficial owner or (b) no natural person is found who exercises control through ownership interest. However, this shortcoming is partly mitigated by the requirements of the Art. 59(1)(2) of the LMML that requires OE to remove any doubt as to who the beneficial owner is.

Art. 63(1)-(3) of the LMML and Art. 38 and Appendix 3 to the RILMML requires the entering in the Commercial Register, the Register of Non-Profit Legal Persons Act and in the BULSTAT Register data and information of the beneficial ownership of the legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria.

Art. 63(4) of the LMML requires the data and information that shall be entered in the Registries under Art. 63(1) of the LMML.

The described data not only allow identification of the BO but also allow identification of the legal persons or other entities where direct or indirect control is exercised over the legal persons or other legal entities (Art. 63(4)(2) of the LMML), as well as allow identification of the natural contact person permanently resident within the territory of the Republic of Bulgaria, where no data on a natural person - legal representative permanently resident within the territory of the Republic of Bulgaria is entered on the record of the legal persons or other legal entities (Art. 63(4)(3) of the LMML.

Further, it is required that any change in the circumstances shall be also entered in the register (Art. 63(4)(4) of the LMML).

Also, the requirements of Arts. 61 and 62 LMML require legal persons, other legal entities, trusts and other legal arrangements to obtain and hold adequate, accurate and current information on the natural persons who are their beneficial owners thereof, and to provide that information to the OEs under Art. 4 LMML (for the purpose of CDD measures applied by the OEs), as well as to the FIU and the other competent authorities (upon request).

(b) Art. 61(1) of the LMML covers the obligation of all legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria and the natural contact persons to obtain, hold and provide adequate, accurate and current information on the natural persons who are the beneficial owners thereof, including the details of the beneficial interests held by the said natural persons. This equally includes an obligation regarding the obligation of the BO of the legal persons and other legal entities established in the territory of the Republic of Bulgaria to provide to these persons and other legal entities or to the natural contact persons all the information necessary for the fulfilment of the obligations of the legal persons and other legal entities and of the natural contact persons under their reporting obligations.

(c) There are a variety of routes that Bulgaria may also obtain beneficial ownership information. In respect of information obtained by financial institutions and/or DNFBPs in carrying out CDD, Art. 61(2) of the LMML provides an obligation for all legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria and the natural contact persons to provide such information to obliged entities under Art. 4 of the LMML (which include both FIs and DNFBPs).

FIs/DNFBPs are required under the LMML to identify the BO and to verify his/her identification (see c.10.5).

In respect of information held by other competent authorities - Art. 74(4) and 74(11), Art. 75(1) and (2), Art. 87, 88 of the LMML and Art. 9(3) and (6), Art. 9a, 9b (1) and (2) of the LMFT allows for the exchange of information between FID-SANS, supervisory authorities, law enforcement authorities, Prosecution and other competent authorities in the cases specified in these laws.

In respect of information held by the company, Art. 61 (3) of the LMML provides an obligation for all legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria and the natural contact persons to provide information on their BO upon request of FID-SANS and other competent authorities.

In respect of available information on companies listed on a stock exchange, Art. 59(4) of the LMML provides an obligation to collect ownership information on any customers which are legal persons listed on a regulated market that are subject to disclosure requirements consistent with European Union law or subject to equivalent international standards, and § 27 of the Transitional and Final Provisions of the LFSC – regarding the obligation of regulated markets to submit to the FSC a list of the individuals, including the beneficial owner.

Criterion 24.7 – Art. 61(1) of the LMML provides for the obligation of all legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria and the natural contact persons to obtain, hold and provide adequate, accurate and current information on their beneficial owners. Art. 63(1)-(3) of the LMML and Art. 38 and Appendix 3 to the RILMML requires the entering in the Commercial Register, the Register of Non-Profit Legal Persons Act and in the

BULSTAT Register data and information of the BO of the legal persons and other legal entities incorporated within the territory of the Republic of Bulgaria.

Art. 63(4)(4) of the LMML requires any changes in the data and information about the BO to be entered too, thus providing for the information and data to be up-to-date (current).

Legal persons and other legal entities are obliged to submit the respective adequate, accurate and current information on their BO for entering in the Commercial Register, the Register of Non-Profit Legal Persons Act and in the BULSTAT Register within 7-days term from their registration in the respective register (Art. 6(2) of the CRRNPLEA and Art. 12(1) of the BRA).

Pursuant to Art. 6(2) of the ACRNPLER and Art. 12(4) of the BRA, the deadline for submission of application for entering any changes in these register (which includes cases referred to Art. 63(4)4 of the LMML) is 7 days after the change.

When the obligation for entering of BO information in the registers was introduced, all legal entities and other legal arrangement were obliged to submit an application for initial entering of the BO information in the registers no later than 31.05.2019. All legal entities registered after 31.05.2019 (the exceptions under Art. 63(5-6) of the LMML apply) are obliged to submit the respective information within 7-days from their registration in the respective register. In any case of change in the entered information an application for entering of the changes is to be submitted within 7 days, pursuant to the general provision of Art. 6(2) of the ACRNPLER and Art. 12(1) and 12(4) of the BRA.

The BO information is entered in the registers upon a notarized declaration signed by the legal person or other legal entity. The template of the declaration is provided in Appendix 3 of the RILMML. According to Art. 118 of the LMML, the sanctions for failing to report/update the BO information to the BO registers are monetary fines, see c.24.13.

Whilst Art. 13 (4) and (5) of the Law on Commercial Register requires submission of a declaration for truthfulness of the stated circumstances and this is equally contained in Art. 9 (4) of the Law on BULSTAT Register, there are no sufficient regulatory measures to ensure (verify) accuracy of the information.

In respect of information held by FIs/DNFBPs, Art. 61(2) of the LMML requires all legal persons and other legal entities incorporated within the territory of Bulgaria and the natural contact persons to provide such information to FIs/DNFBPs. Art. 3(1), Art. 10(2) and Art. 59, 61, 64 and 65 of the LMML and Art. 37-40 and Appendix 2 to the RILMML of the RILMML requires FIs/DNFBPs to identify the BO and to verify his/her identification (see c.10.5). Art. 16 of the LMML requires FIs/DNFBPs to keep this information current.

Criterion 24.8 – Art. 63(4)(3) of the LMML requires the legal entity to record in the relevant register data on a natural contact person permanently resident within the territory of the Republic of Bulgaria if no data on a natural person – legal representative is entered on the record (notarised consent to this recording is required).That person is required by Art.61(3) of the LMML to provide the FID-SANS and competent authorities with beneficial ownership information as outlined in Art.61(1) of the LMML. However, there is no explicit provision for the person to provide further assistance to the competent authorities.

Criterion 24.9 – Art. 3(3) of the LMML and Art. 67(1) of the LMML requires FIs/DNFBPs to keep all documents, data and information collected and prepared for a period of five years. This is calculated from the termination of the business relationship (in case of established business

relationships) and from the completion of the transaction (in case of occasional transactions). The documents must be to be retained so as to be available to FID-SANS, to the relevant supervisory authorities and to auditors. However, this only partly satisfy the criterion as there is no requirement placed on authorities and company itself to maintain the information and records for at least five years after the date on which the company is dissolved or ceases to exist.

Criterion 24.10 – Art. 63(8)(1) of the LMML grants direct access to the FID-SANS and other competent authorities to basic and beneficial ownership information in the respective registrars. That information is then transferable between competent authorities; Art. 61(3) of the LMML provides for the access of the FID-SANS and other competent authorities to beneficial ownership information held by the legal persons established in Bulgaria upon request.

The BULSTAT Register and the Commercial register and Register of Non-Profit Legal Persons (which contain both basic and BO information) are public and the access is unrestricted. All public authorities, including the FIU, and third parties are able to check the information entered therein. There is no requirement for the requestor to demonstrate legitimate interest in order to access the information and there are no mechanisms or obligation provided for the Registry agency to report or inform the entity concerned that such check is done. As far as the registers are electronic, the available information is adequate and current up to the time of the check made. Upon request, the Registry Agency may provide for certified paper copies of the information entered and the documents attached to the legal entities' files.

There are a series of other powers under the LMML for the FID-SANS to request information from state bodies and municipal authorities (Art. 74(4) and (11) of the LMML and Art. 9(3), (6) and (10) of the LMFT); FID-SANS to request all types of information by obliged entities, incl. BO information (Art. 74(1) - (3) and (11) of the LMML and Art. 9(3), (6) and (10) of the LMFT), for FID-SANS to request information for the performance of its supervisory functions (Art. 108(3), 109(1)(2-3) and 4 and Art. 111 of the LMML and Art. 14a of the LMFT) and obligations for obligation for entities under Art. 4 to provide requested information in respect of requests.

Art. 159 of the CCP and Ordinance RD-04-91/07.03.2019 of the Prosecutor General adds that in addition to having access to all public registers, for the needs of the investigation of criminal cases PO may request any documents (Art. 159 CCP) from the Registry Agency regarding the basic and beneficial ownership information. Prosecutors also have the opportunity to receive information and documents that are in the electronic files of commercial entities, outside the publicly accessible part of the Commercial Register, through specially designated in the PO employees with qualified electronic signatures, Ordinance RD-04-91/07.03.2019 of the Prosecutor General.

Criterion 24.11

(a) Legislation provides for elimination of the possibility for the joint stock companies and for the partnership limited by shares to continue to issue bearer shares or substitute interim certificates; Art. 178 of the Commercial Law and §11-14 of the Law on Amendment to the Commercial Law (SG № 88 from 2018, effective from 23.10.2018). In accordance with the Art. 167(1) of the Commerce Act, interim certificates, that can be issued by a Joint-stock company to its shareholders before the issuance of the shares, entitles the shareholders to receive their stocks upon presentation of interim certificates.

(b) Bearer shares issued prior to the entry into force of the law shall be replaced by registered shares. Within nine months of the entry into force of the law, companies that issued bearer shares or substitute interim certificates shall amend their Articles of Association, replace the bearer

shares or substitute interim certificates with registered shares, start keeping Books of shareholders, declare the changes and submit the amended Articles of Association in the Commercial Register for announcing. If a shareholder does not submit the bearer shares owned or substitute interim certificates for replacement, the company invalidates the shares. The companies that do not comply with the abovementioned requirements or have been subject to refusal for recording of the declared changes shall be terminated pursuant to Art. 252(1)(4) of the Commercial Law with decision by the Court upon a request filed by the prosecutor. The already incorporated companies were required to convert bearer shares with registered ones by 23.07.2019.

The Registry Agency monitors the companies that have failed to transform its shares into registered shares; §13 of the Act for amendments in the Commercial Act. However, the Bulgarian authorities confirmed during the AT's onsite visit that there has not been any monitoring process to ensure that bearer shares have been converted to registered shares. Further information received after the onsite visit suggest that 40% of the companies failed to convert bearer shares into the registered shares. More information on the actions taken by the authorities is provided under IO5.

(c) (N/A)

(d) (*N/A)*

Criterion 24.12 – Bulgaria has no mechanisms in place in order to ensure that nominee shares and nominee directors are not misused for ML/TF. There are, however, cases of the abuse of informal nominees in Bulgaria, without a provision to prevent against this.

Criterion 24.13 – Bulgaria has a series of administrative sanctions under Chapter 10 of the LMML that can be imposed on OEs and on any person who manages and represents a FI/DNFBP; for more information on sanctions for non-compliance with the preventive measures by the OEs see analysis under R.35.

Sanctions for non-compliance with the requirements at Art. 61-63 of the LMML on provision of beneficial ownership information are stipulated under Art. 118 of the LMML. These include under Art. 118(1) - fines ranging from BGN 1000 to 10 000 (approx. EUR 500 to 5 000) for legal persons and sole traders; fines ranging from BGN 500 to 5 000 (approx. EUR 250 to 2 500) for natura persons. Fines can be increased for repeated and systemic violations: (i) for natural persons – ranging from BGN 1 000 to BGN 10 000 (approx. EUR 500 to 5 000) for repeated violations and BGN 2 000 to 20 000 (approx. EUR 1 000 to 10 000) for systemic violations; (ii) for legal persons and sole traders - ranging from BGN 2000 to 20 000 (approx. EUR 1 000 to 10 000) for repeated violations and BGN 5 000 to 50 000 (approx. EUR 2 500 to 25 000) for systemic violations; (Art. 118(2), Art. 118(3) of the LMML). In addition, to convince the perpetrator to fulfil his/her obligation for submission of application for entering of BO information, Art. 118(4) of the LMML envisages imposition of sanctions according to Art. 118(1) of the LMML every month until the recording is declared (the application for entering of data is submitted). This is applied in cases in which, after being sanctioned by a fine or by a pecuniary penalty under Art. 118(1) of the LMML for failing to fulfil an obligation to declare a recording under Art. 63(4) of the LMML, the person fails further (or continuously) to declare the said data for recording within the set time limit.

Further, there are also specific sanctions under Art. 118(5) of the LMML for contact persons (BGN 100 (approx. EUR 50) or exceeding this amount but not exceeding BGN 1 000 (approx. EUR 500) and in the case of repeated violation, to a fine of BGN 200 (approx. EUR 100) or exceeding this

amount but not exceeding BGN 2 000 (approx. EUR 1 000). Similarly, penalties can be imposed at Art. 40 of the ACRNPLER and Chapter VI of the BRA for non-executing the obligation for entering basic information and further changes in it in the registers.

The sanctions are not proportionate or dissuasive in all circumstances.

Criterion 24.14

(a) The BULSTAT register and the Commercial register and Register of Non-Profit Legal Persons are public and access is unrestricted. These registers contain both basic and BO information. All domestic and foreign authorities are able to check the information entered therein. There is no requirement for the requestor to demonstrate legitimate interest in order to access the information and there are no mechanisms or obligations provided for the Registry agency to report or inform the entity concerned that such check is done. As far as the registers are electronic, the available information is adequate and current up to the time of the check made.

The Registry agency is currently developing the new system in collaboration with the other EU member states and with the European e-Justice Portal, called BORIS – Business Ownership Registers Interconnection System. The users will access BO Registers in other Member States via the European e-Justice Portal (BORIS) with their own national electronic identification schemes (eIDs). BORIS will allow users to acquire products that are provided by the MS BO registers.

The FID-SANS has the same information gathering powers for the purpose of providing assistance to its foreign counterparts as it has for the performance of its functions for analysis domestically. All documents, data and information available and/or gathered by FID-SANS (from other authorities, obliged entities under Art. 4 of the LMML, legal persons or other legal entities themselves under Art. 61(3) of the LMML, as well as information accessible in the CRRNPLE and the BULSTAT Register) can be and is regularly shared with foreign counterparts.

The BNB information exchange concerns predominantly the fit and proper issues of shareholders/acquisitions in credit institution/other financial institution, observations from AML/CFT inspections or notifications linked with establishing a branch in other EU MS or conducting AML/CFT inspection.

The FSC also exchanges information with wide range of countries. Pursuant to Art. 25(6) FSCA, information constituting professional secret may be provided to a foreign authority of a third country exercising financial supervision. According to the Art. 13(1)(25) of the FSCA, the FSC cooperates with the European Commission, the European Insurance and Occupational Pensions Authority, the European Securities and Markets Authority, the European Banking Authority and the European Systemic Risk Board and provides them the information necessary for the performance of their duties, including the prevention of the use of the financial system for the purpose of money laundering and terrorism financing.

(b) Art. 90(1) and (7) of the LMML and Art. 14 of the LMFT allows international exchange of information performed by the FID-SANS. Art. 74 of the LMML and Art. 9(3) and (6) of the LMFT provides the power for FID-SANS to access information held by obliged entities and state bodies and municipal authorities and the equal powers for FID-SANS, regardless of if the information is needed for the domestic analysis of STR or information on ML/TF or associated predicate offence received from a state body, or for the purpose of answering requests from foreign counterparts.

As outlined in c.24.13, the FID-SANS, BNB and FSC all regularly provide and seek international co-operation which includes information on shareholders.

Please refer also to information provided in c. 29.3 and c. 40.11.

(c) Art. 74 of the LMML and Art. 9(3) and (6) of the LMFT permits the FID-SANS to access information held by obliged entities and state bodies and municipal authorities and the equal powers for FID-SANS, regardless if the information is needed for the domestic analysis of STR or information on ML/TF or associated predicate offence received from a state body, or for the purpose of answering requests from foreign counterparts (please refer also to information provided under c.29.3 and c.40.11).

In response to a European Investigation Order or a request for legal assistance, the competent authorities of the PO may obtain any information by the means referred in c.24.10 on legal and non-profit entities, including beneficial ownership for the provision of foreign states.

The FSC have powers under Art. 13(1)(23-26) and Art. 25(4)-(6) of the FSCA in respect of international co-operation. Art. 257 and 262(2)(1) of the MFIA allows the provision by the FSC of information to competent authorities of EU member states. Art. 258 of the CISOUCIA allows the provision by the FSC of information to competent authorities of EU member states. Art.100z(1) and (3) of the POSA allows for the provision of information by the FSC to competent authorities of EU member states; see also c.37.8 and c.40.8).

Criterion 24.15 – There are no explicit legal provisions for monitoring the quality of assistance in respect of international exchange of beneficial ownership information.

The FID-SANS informed that in practice quality of data received by the FID-SANS from foreign FIUs in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad, is monitored annually while drafting the annual report and is also done on ad-hoc basis (see also Recs 37 and 40).

In the case of the BNB, monitoring assistance is completed for each of cases/instances separately. For the FSC, whilst there is no explicit legal provision for monitoring the quality of assistance, i.e., quality of data received by FSC from foreign counterparts in response to requests for basic and beneficial ownership information, in practice the FSC keeps a database on the data requested and received, and reviews all received data taking into account the quality and timeliness of information provided from requested counterparts and also provides feedback. Additionally, within the IOSCO MMoU (which is the basis for more than half of all FSC's annual requests for international cooperation and exchange of information), all signatories provide annual statistical information related to that MMoU.

Weighting and Conclusion

The following deficiencies apply: (i) Bulgaria has conducted high level risk assessment of legal persons, however, ML/TF risks associated with all types of legal persons have not been comprehensively assessed (c.24.2); (ii) there are no specific provisions in Bulgaria to ensure that basic information required at c.24.4 is always maintained by the companies within the country at a location notified to the companies' registry (c.24.4); (iii) there are not sufficient mechanisms in Bulgaria to ensure accuracy of the basic information (c.24.5); (iv) minor shortcomings concerning BO definition identified at c.10.5 have an impact on criterion c.24.6 (c.24.5); (v) there are no sufficient regulatory measures to ensure (verify) accuracy of the BO information (c.24.7); (vi) authorities and legal persons themselves are not required to maintain the information and records for at least five years after the date on which the company is dissolved or ceases to exist (c.24.9); (vii) Bulgaria has taken steps to legally require bearer shares conversion into the registered shares by mid-2019, however, the exercise has not been completed to date (c.24.11);

(viii) the sanctions for persons that fail to comply with the requirements are not proportionate or dissuasive in all circumstances (c.24.13); (ix) there are no mechanisms in the country to prevent nominee misuse (c.24.12). **R.24 is rated PC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the 2013 MER, the AT concluded that former R. 34 is not applicable to Bulgaria due to the fact that trusts and legal arrangements cannot be legally established in Bulgaria.

Criterion 25.1

(a) *(N/A)* Bulgarian domestic law does not provide for the existence of trusts governed under their law and Bulgaria is not a signatory to the Hague Convention on Laws Applicable to Trusts.

(b) *(N/A)* Bulgarian domestic law does not provide for the existence of trusts governed under their law.

(c) Trustees are obliged entities under the Art. 4(16) of the LMML. Trustee of a trust governed under the foreign law must comply with the CDD, record keeping obligations including the information referred to in (a), i.e., settlor, trustee, protector, beneficiaries, etc. However, trustees are not explicitly required to obtain basic information on other regulated agents of, and service providers to, the trust, including investment advisors and managers, accountants and tax advisors.

Whilst professional trustees could exist in Bulgaria providing services to foreign law trusts, in accordance with the Art. 3(3) of the BRA, there are currently no entries in the BULSTAT Register based on this provision.

Criterion 25.2 – Bulgarian domestic law does not provide for the existence of trusts governed under their law. With regard to trusts and other similar foreign legal arrangements that may operate within the territory of the Republic of Bulgaria, the provisions of Art. 3(3) of the BRA and of § 2 (1) p.2 of the LMML shall apply.

Art. 62(1) of the LMML applies regarding the obligation of natural and legal persons and other legal entities which operate within the territory of the Republic of Bulgaria in their capacity of trustees of trusts, escrow funds and other similar foreign legal arrangements incorporated and existing under the law of the jurisdictions providing for such forms of trusts, and the natural contact persons (referred to in Art. 63(4)(3) of the LMML) to obtain, hold and provide adequate, accurate and current information on the beneficial owners (BO) of the trust.

Art. 63(1) - (3) of the LMML and Art. 38 and Appendix 3 to the RILMML requires information to be entered on the BULSTAT Register of data and information of the BO. Art. 63(4) of the LMML provides a list of the data and information that shall be entered in the BULSTAT Register.

The definition of Beneficial owner in respect of Trusts is contained in § 2 of the Supplementary Provisions to the LMML and covers any natural person or persons who ultimately owns or controls a legal person or other legal entity, and/or any natural person or natural persons on whose behalf and/or for whose account an operation, transaction or activity is being conducted. In respect of trusts and legal arrangements it states that the beneficial owners shall be considered to be (a) the settlor; (b) the trustee; (c) the protector, if any; (d) the beneficiary or the class of beneficiaries, or (e) the person in whose main interest the trust is set up or operates, where the individual benefiting from the said trust has yet to be determined; (f) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

Art. 3(1), Art. 10(2) and Art. 59, 61, 64 and 65 of the LMML and Art. 37-40 and Appendix 2 of the RILMML requires FIs/DNFBPs to identify the BO and to verify information. Art. 16 of the LMML requires FIs/DNFBPs to keep the information collected through due diligence measures current. Deficiencies identified under sub- criterion 10.7(b) apply here.

Criterion 25.3 – There is no obligation for trustees to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction.

Criterion 25.4 – Trustees are not prevented by law or other enforceable means from providing competent authorities with any information relating to the trust.

Criterion 25.5 – Trustees of a foreign law trust operating in the territory of Bulgaria are required to provide BO information to the FID-SANS and other competent authorities upon request by a prescribed deadline (Article 62(3) of the LMML) and where trustee services are provided by the way of business (incl. those that act or arrange another person to act as a trustee) trustees are OEs under Art. 4(16) of the LMML. This provides for information to be shared to the BULSTAT Register and the availability of the information to the competent authorities. The powers of the competent authorities referred to under Recommendations 27, 29 and 31 apply. In addition, the provisions of Art. 3(3) of the BRA and of § 2(1)(2) of the LMML shall apply. However, there is currently no legal mechanism in place to identify those who are conducting trustee services and therefore the population of trustees is unknown. For this reason, the authorities are unable to identify trustees and thereby obtain timely access to information from trustees.

Criterion 25.6

(a) Public access to the BULSTAT Register is granted under Art. 8, Art. 36 and Art. 37 of the Law on the BULSTAT Register; that means that the need for direct contact for information is limited. BULSTAT Register and the Commercial register and Register of Non-Profit Legal Persons are public, and access is unrestricted. These registers contain both basic and BO information. All competent authorities are able to check the information entered therein. There is no requirement for the requestor to demonstrate legitimate interest in order to access the information and there are no mechanisms or obligations provided for the Registry agency to report or inform the entity concerned that such check is done. As far as the registers are electronic, the available information is adequate and current up to the time of the check made. Domestic competent authorities exchange this information with foreign counterparts upon request. Registry agency is currently developing the new system in collaboration with the other EU member states and with the European e-Justice Portal, called BORIS – Business Ownership Registers Interconnection System. The users will access BO Registers in other Member States via the European e-Justice Portal (BORIS) with their own national electronic identification schemes (eIDs). BORIS will allow users to acquire products that are provided by the member states BO registers.

(b) Art. 74 of the LMML and Art. 9(3) and (6) of the LMFT grants powers to FID-SANS to access information held by obliged entities and state bodies and municipal authorities, regardless of if the information is needed for the domestic analysis of STR or information on ML/TF or associated predicate offence received form a state body, or for the purpose of answering requests from foreign counterparts.

The FSC has powers under Art. 13(1)(23-26) and Art. 25(4)-(6) of the FSCA in respect of international co-operation. Art. 257 and 262(2)(1) of the MFIA allows the provision by the FSC of information to competent authorities of EU member states. Art. 258 of the CISOUCIA allows

the provision by the FSC of information to competent authorities of EU member states. Art. 100z(1) and (3) of the POSA allows for the provision of information by the FSC to competent authorities of EU member states (see also Criterion 37.8 and Criterion 40.8). Further as regards the BNB's activity towards banks, PIs and EMIs, it will process a request from foreign competent authority based on provisions of art. 65-66, 87-88 of LCI and Art. 160-160a of LPSPS.

(c) In response to a European Investigation Order or a request for legal assistance, the competent authorities of the PO may obtain any information by the means referred in c.24.10 on legal arrangements, including beneficial ownership for the provision of foreign states.

Criterion 25.7 – Trustees as OEs under the LMML are subject to sanctions analysed at R.35. Shortcomings identified at R.35 apply here.

In addition, Art. 40 of the ACRNPLER and Chapter VI of the BRA provides for the penalties imposed for non-executing the obligation for entering basic information and further changes in it in the registers. The penalties are not proportionate or dissuasive in all situations due to their relatively low level (range BGN 100 – 1 000, approx. € 50 -500).

Criterion 25.8 – Whilst trustees as OEs under the LMML are subject to sanctions analysed at R.35, there are no explicit sanctions for professional trustees for failing to grant timely access to competent authorities to information referred to in c.25.1.

Weighting and Conclusion

The following deficiencies apply: (i) professional trustees of foreign law trusts are not required to disclose their status to FIs/DNFBPs when forming a business relationship or carrying out an occasional transaction; (ii) no explicit power is provided in the legislation for to allow competent authorities to use their investigative powers to obtain beneficial ownership information on behalf of foreign counterparts; (iii) sanctions applicable to trustees for failure to meet their obligations in relation to CDD, record keeping and providing information to the registry are not considered to be fully dissuasive and proportionate; (iv) there are no explicit sanctions for professional trustees for failing to grant competent authorities timely access to information. **R.25 is rated PC**.

Recommendation 26 – Regulation and supervision of financial institutions

In the 2013 MER, Bulgaria was rated LC with former R.23. The assessment identified technical deficiencies related to market entry controls for the exchange bureaux.

Criterion 26.1 – Art. 108(1-2) of the LMML and Art. 14a of the LMFT designate the FID-SANS as the main control authority responsible for ensuring that OEs comply with the AML/CFT requirements.

Further, Art. 108(6) of the LMML establishes that control of compliance with some provisions under LMML (that excludes STR reporting requirements) shall be exercised using a risk-based approach by the BNB, the FSC and the NaRA over entities operating in gambling sector. This includes both, off-site and onsite supervision. Art. 9A(2) of the LMFT requires supervisory authorities to verify compliance with the requirements of LMFT (that includes CTF and TFS related to TF) by the OEs, with violations being informed immediately to FID-SANS.

In addition, Art. 79 of the LCI and Art. 154 (1), (2) and (6) of the LPSPS (regarding banks and payment supervision) permit the BNB, in its capacity as supervisor of credit institutions and other payment service providers to exercise supervisory powers for AML/CFT purposes. Art. 12 of the

FSCA permits the FSC, in its capacity as supervisor of the securities (investments), insurance and pension sectors, to exercise supervisory powers for AML/CFT purposes.

In addition to the listed supervisory authorities, Art. 108(7) of the LMML establishes that supervision may furthermore (i.e., FID-SANS is the primary supervisor) be conducted by other supervisory authorities which, according to §1(11)) means the State bodies empowered by a law or another statutory instrument act to exercise general supervision over the activities of OEs. However, it is not clear who these authorities are, as the LMML does not name them.

Although in practice such other supervisory authorities are the NaRA regarding currency exchange and the CRC regarding postal money operators (see IO3 for more information), the legal basis for this supervision has not been established.

Criterion 26.2 – All Core Principles FIs are required to be licenced as follows: credit institutions under Art. 13 of the LCI; investment services (securities) under Art.17 of the MFIA; collective investment schemes under Articles 12 and 95 of the CISOUCIA; insurance operators and intermediaries under Articles 28 and 296 of the IC.

Other FIs: 'Other payment service providers' are licenced under Articles 7 (regarding payment institutions) and Art 36(1) (regarding e-money institutions) of the LPSPS and postal operators that handle postal money orders are licensed by the CRC under Art. 39 of the Postal Services Act. Currency exchange offices are required to be entered in a public register maintained by the NaRA prior to the commencement of business, according to Ordinance No. 4.

Some financial services fall outside the scope of regulatory regime, i.e., are not subject to licensing and supervision with AML/CFT requirements. These are paper-based vouchers and paper-based traveller's cheques (except where carried out by bank) and safekeeping. The shortcoming regarding paper-based vouchers and cheques, although concerning as these may be vulnerable to ML/TF abuse due to anonymity features, is weighted moderately heavily as these are not common means of payment in Bulgaria, according to the statistics provided by the authorities. The severity of the regulatory shortcoming regarding safekeeping is to some extent mitigated by the fact that safes offered by the banks fall under the regulatory regime. However, safekeeping related exemption is still considered significant due to a prevalence of ML cases in which unlicensed safe deposits feature, thus is weighted heavily.

Shell banks: The LCI and BNB Ordinance No. 2 prohibit the establishment of shell banks through requirements for licensing which include, at Articles 7 and 10 of the LCI, that the bank should have a physical presence in Bulgaria and should be managed and represented by at least two persons at its registered office.

Criterion 26.3 – FIs are subject to varying levels of entry controls under the relevant legislation, as set out below. In no cases do the legal requirements or regulatory measures explicitly prevent licensing where relevant individuals are associated to criminals.

The legal terminology regarding persons with criminal convictions differs across the various laws listing entry control requirements regarding the type of offences that are prohibited ("pre-meditated", "deliberate", etc.) and applicable rehabilitation rules, as summarised below. Except for qualifying shareholding in pension insurance companies, under the SIC, crimes of negligence are not a barrier to entry. It is the AT's view that rehabilitation is easily achievable.

Art 108(8) LMML requires FID-SANS to carry out offsite inspections regarding requirements under Art. 105 of the said law which prohibits persons who have been convicted of an intentional

crime of general nature, unless rehabilitated, in so far as a law does not provide otherwise from being procurator, manager, member of a management or supervisory body or a general partner in a legal advisor, TCSP service provider or real estate agent.

Credit institutions: BNB licensing prohibits, under Art. 11 of the LCI, members of the management board or board of directors from having "conviction for a premeditated offence at public law, unless he has been exonerated, and, under Art. 14, shareholders controlling more than 3 per cent of the votes must not "harm the reliability or security of the bank or its operations". According to Art. 18 of the BNB Ordinance 2, any person that intends to acquire holding in the capital of a bank licensed by the BNB has to be approved; an approval under Art. 28 or Art. 31 of the LCI is required for such a person. Art. 28 of the LCI requires prior approval in cases where the holding would be in excess of 20 per cent or it becomes a "qualifying holding" within the meaning of Article 4(1)(36) of Regulation (EU) No. 575/2013, which is 10 per cent or more.

Further, BNB Ordinance No. 2 requires that natural persons with more than 3 per cent of the votes must provide declarations of any penalty regarding tax evasion or previous convictions and Ordinance No. 2 requires that board members must complete a "Fit and Proper Questionnaire" which could give grounds for refusal.

Art. 6(10) of Ordinance No. 2 requires shareholders to submit the names and addresses of 'connected persons' (family and business associates) as defined at § 1(4) LCI. Although this information might be to some extent relevant for detection of the close associates, it is not explicit that such information is grounds for a refusal.

Although the BNB complies[112] with EBA Guidance on the suitability of shareholders, the requirements of it are aimed at guiding the country in the fitness and propriety assessment process and do not provide a clear legal basis for establishing specific requirements on how the country implements them, nor does it provide clear legal basis for refusing a licence. Moreover, the implementation of guidance cannot be strictly enforced under the EU 'comply or explain' mechanism; also, although the LCI makes a reference to the EBA guidelines (a general reference without specifying which specific guidelines are applicable in these cases), it also provides the possibility for the BNB not to apply them.[113] Furthermore, the guidance states that suitability assessments *should* (not *must*) include close associates, further suggesting that regulatory processes should be established at the country level on how the assessment of the close associates should be carried out rather than the guidelines alone prescribing this.

The BNB and the ECB cooperation mechanism applies to licensing of credit institutions established in Bulgaria. This provides for a level of mitigation regarding licensing / approval, change of qualifying holdings of the credit institutions[114].

Regarding acquisitions of shareholdings, Art. 28(1) of the LCI establishes that prior written approval of the BNB is requires to acquire, directly or indirectly, a qualifying shareholding Art. 28a(3) requires BNB assessment of the application with a view to ensuring its future sound and

[112] AT is advised that the BNB Governing Council has taken a decision to comply with these guidelines under Art. 79A(2) of the LCI.
[113] Art. 79A(2) of the LCI also provides for cases where EBA guidelines, recommendations and other measures are not complied with (when there are "reasonable grounds" stated under the so called "comply or explain" mechanism).
[114] The ECB is in charge of the authorisation (licensing) procedures in Bulgaria, after establishing a close cooperation mechanism with the BNB.

reasonable management, including consideration of the reputation of the applicant as well as ML/TF risk.

Further to the legal provisions summarised above, the AT is advised that the BNB complies with EBA Guidance on the assessment of suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU and with joint guidelines issued by ESA. Although Art. 79A(2) of the LCI requires the BNB to follow EBA Guidance, this is not considered to be law or enforceable means; please also see above justification.

Securities: FSC licensing prohibits, under Art. 13 of the MFIA, members of the management board or board of directors from having "conviction for a premeditated offence at public law" and, at Art. 157, requires consideration of "reputation" of persons holding a holding of over 10 per cent. Art. 53 of the MFIA prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding without prior FSC approval. Art. 57(1) of the MFIA requires the FSC to assess the application to ensure stable and prudent management, including consideration of the reputation of the applicant as well as ML/TF risk. The following shortcoming applies here: no explicit non-criminality requirement for managers and shareholders.

Collective investment schemes: FSC licensing prohibits, under Art. 10 of the CISOUCIA, a person elected as a member of the board of directors from having "been convicted of crimes against property, economic offences or offences against the financial system, the tax system or the social insurance system, committed in Bulgaria or abroad, unless rehabilitated" and, under Art. 93, a persons who is elected to be a member of a managing or controlling body of a management company shall not have been "convicted of premeditated crime of general nature, unless rehabilitated".

Art. 224(1) of the CISOUCIA prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding (10 per cent) without prior FSC approval. Art. 224(2) requires the FSC to consider the application in accordance with Articles 53-57 and 59 of the MFIA thereby including consideration of reputation and ML/TF risk.

Insurance operators and intermediaries: FSC licensing requires, under Art. 67(7) of the IC, persons holding a qualifying interest of 10 per cent to be persons of "good reputation" and Art. 80 prohibits such persons from having been "convicted of a deliberate criminal act of general nature". Art. 68 (1) of the IC prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding without prior FSC approval; Art. 68(7) requires the FSC to assess the application to ensure suitability and financial stability, including consideration of the reputation of the applicant as well as ML/TF risk. The following shortcomings applies here: no requirement regarding non-criminality of managers.

Pension insurance: FSC licensing requires, under Art. 121e of the SIC, that the members of the management and the supervisory body of the retirement insurance company or of the board of directors, the other persons authorised to manage it or represent it, as well as the persons who perform managerial functions in the company "have good reputation and integrity" and prohibits such persons from having been "convicted for a premeditated offence at public law. Art 121g requires that persons with a qualifying shareholding (10 per cent or more) not be subject of "data based on which it could reasonably be assumed" that ML/TF "is or was perpetrated or intended to be perpetrated in relation to the acquisition, or that the implementation of the acquisition applied for would increase such risk" and requires such person to be "of good standing".

Art. 121g(3) of the SIC prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding without prior FSC approval; Art. 121g(1) requires an applicant to satisfy the requirements of Art. 121e(5) which includes prohibition of persons with criminal conviction as well as for crimes of negligence unless where rehabilitated.

Other payment service providers (PIs/EMIs): Entry controls regarding payment institutions and e-money institutions are established under the LPSPS and Ordinance No. 16 of the BNB. Art. 10(4)(9) of the LPSPS requires the persons managing and representing the entity to satisfy requirements regarding "fitness and probity". Art. 10(4)(10) of the LPSPS requires persons with a qualifying holding within the meaning of Article 4(1)(36) of Regulation (EU) No. 575/2013, which is 10 per cent, to be suitable to "ensure the sound and prudent management of the payment institution". Art. 12(4) of the LPSPS requires the institution to comply with these requirements throughout the licenced period. Art. 37 of the LPSPS applies the above detailed requirements to e-money institutions. Art. 14(1) of the LPSPS prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding without prior BNB approval. Art 14(5) of the LPSPS requires the BNB to assess the application to ensure suitability and financial stability, including consideration of the reputation of the applicant as well as ML/TF risk.

Ordinance No. 16 of the BNB provides further detail regarding the licensing procedure including, at Articles 4-7a regarding payment institutions and Articles 24-27a regarding e-money institutions. Both include that person with a qualifying holding must provide information regarding probity, including convictions status certificate and questionnaire declaration. Art. 4(1)(3) prohibits managers, representatives and members of management and supervision bodies from being persons who have been convicted of a premediated crime of general nature, unless rehabilitated. The following shortcoming applies here: there is no explicit requirement regarding non-criminality of beneficial owners.

Currency exchange: Art. 10 of Ordinance No. 4 provides that no entry shall be made in the register and the entry made shall be deleted ex officio in cases where individual traders, members of the management and supervisory bodies and unlimited partners in the legal entities have been convicted of an "intentional crime of general nature. Art. 6(2)(7) requires the applicant for registration to provide a document for establishing the circumstances regarding the criminal records of the individuals. The entry controls do not extend to beneficial owners.

Postal operators handling postal money orders (PMO): Chapter Five of the Postal Services Act details the licensing procedure. There are no entry controls regarding the fitness and propriety of owners, controllers or managers of postal operators, although the CRC may refuse a licence under Art. 47(2)(1) or suspend or terminate a licence under Art. 55(1)(2) of the Postal Service Act in cases where there are circumstances that "threaten the security and defence of the country as per an opinion" of SANS or the MOD (although there is no legal requirement to consult with these authorities).

Other FIs

Other FIs that are conduct the following activities - financial leasing, guarantee transactions, acquisition of accounts receivable on loans and other type of financing (factoring, forfeiting, etc.) are registered under Art. 3(a) of the LCI. They shall be entered into a public register of the BNB if one or more of the activities are carried out by occupation. Requirements for registration (Art. 3a(2)) include that the persons managing and representing the company shall have the necessary qualification, professional experience and reputation, and the persons which directly or indirectly have a qualifying share participation in the capital of the company shall have the necessary

credibility, financial stability and reputation. Art. 5 of BNB Ordinance 26 establishes additional requirements for the management and owners of 'Other FIs', including persons managing and representing as well as those holding qualifying shareholding shall not be convicted of a premeditated crime of general character, unless rehabilitated. The BNB shall delete an 'Other FI' from the register in cases where it does not fulfil its obligations under any statutory requirements, thereby including compliance with AML/CFT laws under Art.3a (6) of the LCI.

Criterion 26.4

Basel Committee on Banking Supervision (BCBS) Principles

The IMF/World Bank conducted a Financial Sector Assessment Programme (FSAP) in 2015 and published a Technical Note regarding progress made in 2017. The 2017 Technical Note included further short (during 2017), medium (during 2018) and long term (during 2019) targets in order to achieve compliance with the principles. The current levels of compliance have not been re-evaluated by IMF/World Bank; however, annual reports of the BNB reflect further progress made since 2017.

International Association of Insurance Supervisors (IAIS) Principles

Authorities reported that the IMF/World Bank technical note of 2017 included consideration of IAIS principles, however, this does not appear to be the case.

International Organization of Securities Commission (IOSCO) Principles

Authorities reported that the assessment was recently carried out by EIOPA and ESMA of the independence of national competent authorities, including Bulgaria. The resulting EBA, EIPPA and ESMA reports provide aggregated results rather than country-specific results.

Based on the additional information that was made available to the AT by the authorities, supervision is mostly in line with applicable core principles.

Other financial institutions:

While the BNB has risk-based systems in place to monitor and ensure compliance by the EMIs and PIs with the national AML/CFT requirements, regulation and supervision of all other FIs (outside core principles institutions and PIs/EMIs) demonstrates notable shortcomings and does not appear to have regard to the ML/TF risks in these sectors.

Regulation and supervision of currency exchange providers by the NaRA and postal money operators by the CRC is not risk based and systems for supervisory monitoring are underdeveloped. These shortcomings are material due to the risk exposure and vulnerabilities of the currency exchange and PMOs sector, see Chapter 1 for more information.

Criterion 26.5 – Art. 114(1) of the LMML requires that supervisory activities shall be carried out applying a risk-based approach. It specifies that this shall consist of: (1) identification of the relevant risk factors by collecting the necessary information, including with respect to risks associated with customers, products and services; (2) use of the information collected to assess and understand the ML/TF risks as well as the measures taken reduce and mitigate the said risk; (3) taking measures for the implementation of control activities proportionate to the said risks and allocation of resources in accordance with the risk assessment, including making decisions on the scope, depth, duration and frequency of the on-site inspections, as well as on the need of human resources and expertise for the implementation of the control activities; (4) ongoing monitoring and periodic review of the risk assessment and of the allocation of resources for the

implementation of the control activities, including upon the occurrence of essential circumstances or changes in the management and activities of the OE so as to ensure that the risk assessment and resource allocation are current, applicable and relevant. Furthermore, Art. 115 requires all supervisors to take national and supranational risks into account when carrying out risk assessments.

Whilst the above addresses sub-criterions 26.5(a) and 26.5(b), it does not explicitly cover sub-criterion (c). It is not explicit that data discussed at c.26.5(a) and c.26.5(b) is used by the supervisory authorities with a view to determine the frequency and intensity of the on-site and off-site supervision.

The absence of compliance with c.26.5(c) is a material shortcoming as it requires supervisory authorities to develop characteristics (risk profiles) of the supervised institutions and groups in order to enable allocation of risk based supervisory measures. In light of compliance with only sub-criterions (a) and (b) which require supervisors to take into account country risks and internal controls of OEs, it is very unlikely that supervisors will have a good basis to make an informed decision on overall risk exposure of the OEs.

In addition, it is not explicitly stated that the above listed criteria should be cumulatively used to determine the frequency and intensity of the on-site and off-site supervision.

The BNB reports that it complies with EBA guidance on risk-based supervision which does relate to the requirements of criterion (c) however the EBA guidance documents are not considered to be law or enforceable means.

The BNB (for banks and PIs/EMIs), FSC (for securities and insurance) and the FID-SANS (for some sectors) has provided internal documents on supervisory methodologies clarifying aspects of risk-based approach to supervision (please see IO 3 for more information). No additional documents of a similar nature have been provided by the NaRA or the CRC.

Criterion 26.6 – Art. 114(1)(4) of the LMML requires ongoing monitoring and periodic review of the risk assessment and of the allocation of resources for the implementation of the control activities, including upon the occurrence of essential circumstances or changes in the management and activities of the OE to ensure that the risk assessment and resource allocation are current, applicable and relevant. However, except for the BNB, supervisors are not explicitly required to assess the ML/TF risk profile of an individual financial institution or group, including the risk of non-compliance. The BNB assesses such under BNB-SSAD's Operational Rules and Procedures.

Weighting and Conclusion

The following **minor** shortcoming exists: (i) supervisors are not explicitly required to assess the ML/TF risk profile of an individual financial institution or group, including the risk of non-compliance (c.26.6), (ii) Entry controls of all FIs do not explicitly prevent licensing /registration in case of association with criminals.

The following **moderate** shortcomings exist: (i) Some financial services fall outside the scope of licensing and supervision: paper-based vouchers and paper-based traveller's cheques (except where provided by a bank) and safekeeping (c.26.2); (ii) Number of various other shortcomings established in licensing requirements relate to the absence of explicit requirements regarding non-criminality, as well as rehabilitation, etc. (c.26.3); (iii) Due to multiple shortcomings under c.26.5 these are collectively considered moderate: there is no explicit requirement to determine

frequency and intensity of supervision on the basis of characteristics of the FIs and financial groups, incl. diversity, number, etc. Moreover, it is not explicit that the above listed criteria should be cumulatively used to determine the frequency and intensity of the on-site and off-site supervision (c.26.5); In addition, it is not explicit that data discussed at c.26.5(a) and c.26.5(b) is used by the supervisory authorities with a view to determine the frequency and intensity of the on-site and off-site supervision.

Severe shortcoming exists: Regulation and supervision of FIs (that fall outside the scope of core principles institutions and PIs/EMIs) demonstrates notable shortcomings and does not appear to have regard to the ML/TF risks. Moreover, regulation and supervision of currency exchange providers by the NaRA and postal money operators by the CRC is not risk based and systems for supervisory monitoring are underdeveloped (c.26.4). Consequently, **R. 26 is rated PC**.

Recommendation 27 – Powers of supervisors

In the 2013 MER, Bulgaria was rated C with old R.29.

Criterion 27.1 – The FID-SANS is the main control authority responsible for ensuring OEs compliance with the AML/CFT requirements, according to Art. 108(1) of the LMML and Art. 14a of the LMFT.

Art. 108(6) of the LMML establishes that control of compliance with some provisions under LMML (that excludes STR reporting requirements) shall be exercised using a risk-based approach by the BNB, the FSC and the NaRA over entities operating in gambling sector. This includes both, off-site and onsite supervision.

Art. 9A(2) of the LMFT requires supervisory authorities to verify compliance with the requirements of LMFT by the OEs, with violations being informed immediately to FID-SANS. Measures under LMFT include (Art. 3, 4b) compliance with UNSC resolutions regarding TFS related to TF. In addition, Art. 79 of the LCI and Art. 154 (1), (2) and (6) of the LPSPS (regarding banks and payment supervision) permit the BNB, in its capacity as supervisor of credit institutions and other payment service providers to exercise supervisory powers for AML/CFT purposes. Art. 12 of the FSCA permits the FSC, in its capacity as supervisor of the securities (investments), insurance and pension sectors, to exercise supervisory powers for AML/CFT purposes.

Art. 115(4) of the LMML requires the control authorities to cooperate and exchange information with each other.

Further, RILSANS requires that FID-SANS receive, store, examine, analyse and disclose information collected regarding OEs compliance with the LMML, LMFT, LSANS and Acts regarding their implementation such as RILMML.

Criterion 27.2 – Art. 108(3) of the LMML requires FID-SANS officials to carry out on-site inspections of the application of measures by OEs for the prevention of the use of the financial system for the purposes of money laundering, as well as whenever there is a suspicion of money laundering. Inspections by the FID-SANS may be carried out jointly with the supervisors, according to Art. 108(4) the LMML. The procedure for carrying out the said inspections shall be established by joint instructions of the Chairperson of the SANS and the heads of the supervisory authorities. Art. 108(6) of the LMML establishes that control of compliance with some provisions under LMML (that excludes STR reporting requirements) shall be exercised using a risk-based approach by the BNB, the FSC and the NaRA over entities operating in gambling sector. This

includes both, off-site and onsite supervision. Although Art. 108(7) also requires other supervisory authorities than the ones mentioned above, to carry out inspections over compliance with the LMML, the Law does not name these authorities and laws governing activities by those authorities do not include AML/CFT supervision. Thus, the legal basis for supervision, incl. on-site inspections by NaRA (regarding currency exchange) and CRC (regarding postal operators) is not explicitly established.

For TFS related to TF supervision please refer to c.27.1.

Criterion 27.3 – Art. 109 of the LMML provides FID-SANS and other supervisory authorities (the BNB, FSC and NaRA over gambling) the following rights: unimpeded access to office premises of the person inspected; to require and collect documents, references, excerpts and other information; to require and collect copies of authenticated documents; to require written and oral explanations of relevant circumstances; to set a time limit for the submission of documents, references, excerpts, information and explanations. Art. 110 of the LMML requires the person inspected to comply with such requests and failure to comply constitutes a failing to which penalties apply, according to the Art. 116 of the LMML. See R.35 for more information on sanctions.

Regarding compulsion of information regarding compliance with LMFT (on TF and TFs), Art. 14a LMFT states that control shall be conducted by FID-SANS in accordance with the procedures established under Chapter Nine of the LMML, including the inspections powers detailed above, thus the FID-SANS has the same powers to compel information required to verify compliance with the LMFT as with the LMML. Art. 9a(2) LMFT provides for TF and TFS oversight by the other supervisory authorities, however, this does not include powers to compel information, except the BNB whose power to compel information required for supervision with the LMFT requirements is granted under Art. 80(3) of the LCI.

Criterion 27.4 – The powers of the supervisory authorities to impose sanctions for AML/CFT breaches are discussed in detail at R.35. The range of sanctions include administrative penalties for both, legal and natural persons, regulatory measures to impose warnings, suspend senior managers from executing their duties for a period up to one year, as well as withdraw a licence; suspension of a licence is also possible in certain cases (see also R.35). Deficiencies identified under R.35 have impact on this criterion.

Weighting and Conclusion

The following deficiencies exist: (i) The legal basis for supervision, incl. on-site inspections by NaRA (regarding currency exchange) and CRC (regarding postal operators) is not explicitly established (c. 27.2); (ii) LMFT does not include provisions to compel production of information regarding compliance with LMFT by the supervisory authorities other than FID-SANS and BNB (c. 27.3); (iii) Per R.35: proportionate and dissuasive sanctions for non-compliance with LMML and LMFT are not available in all cases (c. 27.4).

Consequently, **R. 27 is rated PC.**

Recommendation 28 – Regulation and supervision of DNFBPs

In the 2013 MER, the Republic of Bulgaria was rated PC with former R.24. The assessment identified technical deficiencies related to source of funds requirements and ownership thresholds regarding casinos.

Criterion 28.1 – The preventative measures of LMML apply to "obliged entities", which are defined at Art. 4 of the LMML and include both FIs and DNFBPs. Listed at item 21 are the organisers of gambling games, licenced to organise gambling games within the territory of the Republic of Bulgaria pursuant to the Gambling Act.

(a) Licensing of casinos and gambling entities

"Gambling" is defined at Art. 2 of the Gambling Law as "a game of chance whereupon a wager is made and there may be either a winning or a loss of the wager". Matters regulated under the Act include the issuing, extending, revocation and termination of licences regarding the organisation of gambling games and of gambling equipment.

Art. 3 prohibits persons from conducting gambling activities without the proper licence issued by the Director or Deputy Director of the NaRA. Sanctions provided for at Art. 96(1) are monetary fines and range from BGN 5 000 (approx. EUR 2 500) for a person who supports or intermediates up to BGN 2 000 000 (approx. EUR 1 00 000) for a gambling company organising online betting, which could be doubled if a repeat breach is identified.

(b) Gambling licence entry controls

Art. 8 of the Gambling Law lists scenarios whereby a licence shall not be granted which includes where an owner, partner or shareholder with qualified interest (33 per cent), manager, member of a management or controlling body of a company or non-profit legal entity have been found guilty of a crime except where officially rehabilitated.

The ownership threshold is higher than required by the FATF Standard and market entry controls do not cover checks on criminal associations.

(c) Gambling AML/CFT supervision

Art. 108 of the LMML designates FID-SANS as the control authority responsible for ensuring that OEs comply with the AML requirements and Art. 14a of the LMFT regarding TF and TFS requirements.

Art. 108(6)(3) of the LMML introduces the National Revenue Authority (NaRA) as the supervisor for gambling entities.

Art. 9A(2) LMFT requires supervisory authorities to verify compliance with the requirements of the LMFT by the OEs, with violations being informed immediately to FID-SANS. Measures under the LMFT include (Art. 3, 4b) compliance with UNSC resolutions regarding TFS related to TF.

The shortcomings regarding gambling sector, namely entry controls not applied until 33 per cent ownership, and lack of entry controls regarding criminal associates are considered material due to Bulgarian context; Well publicised bribery case, subsequently resulting in resignation of the Chairman of the SCG and dissolvement of the former regulatory authority.

Criterion 28.2 – Art. 108(1-2) of the LMML designates FID-SANS as the control authority responsible for ensuring that OEs comply with the AML/CFT requirements. As described in c.22.1, "Obliged entities" as listed in Art. 4 are broadly equivalent to the FATF definition of DNFBP (see c.22.1 for details).

Criterion 28.3 – All categories of DNFBPs are subject to systems for monitoring compliance with AML/CFT requirements set out under the LMML, RILSANS and LMFT.

As established at c.27.2, Art. 9A(2) of the LMFT requires supervisory authorities to verify compliance with the requirements of LMFT by the OEs, with violations being informed immediately to FID-SANS. Measures under LMFT include (Art. 3, 4b) compliance with UNSC resolutions regarding TFS related to TF.

Criterion 28.4

(a) FID-SANS supervisory powers under LMML and LMFT described under R.26 and R.27 are equally applicable to all categories of DNFBPs.

(b) Art. 105(1) of the LMML states that a natural person as well as a procurator, manager, member of a management or supervisory body or a general partner in listed services (real estate agent, legal advice, TCSP services) shall not be a person who has been convicted of an intentional crime of general nature, unless rehabilitated, in so far as a law does not provide otherwise. This prohibition does not cover beneficial ownership as required by the Standard. Relevant entry controls regarding licensing or registration of DNFBPs are summarised as follows-

Real estate agents: The real estate sector is not subject to licensing and registration requirements and does not have an effective self-regulating mechanism. However, Art 105(1) of the LMML described above applies.

Dealers in precious metals and stones: As explained under c.22.1 such entities are not OEs.

Lawyers, notaries, other independent legal professional and accountants

Lawyers: Art. 3(3) of the Bar Act provides that an attorney-at-law must be registered in the register of the Bar Association. Art 3(5) prohibits the registration of an individual sentenced as adult to imprisonment for a public prosecution of a criminal offence. Art 105(1) of the LMML described above also applies.

Notaries: Art. 2(2) of the Notaries and Notarial Practice Act provides that only persons entered in the Register of the Notary Chamber of Bulgaria may practise as notaries. Art. 8(1) prohibits the registration of persons with record of sentences imposing a penal sanction of deprivation of liberty for a premeditated criminal offence, irrespective of whether they have been rehabilitated or not.

Auditors: Art. 12(1) of the Independent Financial Audit Act provides that the Commission for Public Oversight over Registered Auditors is responsible for oversight of registered auditors. Art 13(1) states only a person with good reputation can apply to become a registered auditor.

Accountants: The Accountancy Law does not provide for licensing or registration; however, Art. 17(1) provides that persons who draw up interim, annual and consolidated accounts of enterprises shall have not been convicted of an indictable offence.

Trust and company service providers: TCSPs are not subject to licensing and registration requirements. Bulgarian authorities advised that such activities are usually performed by lawyers and accountants.

The entry controls described above do not include criminal association or impose conditions regarding the ownership, control or management of firms providing such services.

(c) Further details of sanctions can be found at R.35. Shortcomings identified under R.35 apply.

Criterion 28.5 – Art. 108(6) of the LMML requires the supervisors to carry out supervision using a risk-based approach and specifically includes at Art. 108(6)(3) the NaRA regarding gambling.

The FID-SANS internal procedures for DNFBP risk-based supervision are under development and such analysis of risk is carried out with supervision planned on the basis of information received from other departments of the directorate, from other supervisory bodies and also on the basis of the presence of negative information. In the absence of formalized regulatory processes, it cannot be demonstrated that the frequency and intensity of AML/CFT supervision is determined on the basis of ML/TF risks, characteristics and profiles of the DNFBPs and assessment of adequacy of the AML/CFT controls adopted by the DNFBPs.

Regarding gambling a Joint Instruction on the Terms and Procedure for Conducting Joint On-the-Spot Checks exists between FID-SANS and the NaRA. However, the Instruction does not include division of responsibility or any requirements regarding scheduling and extent of supervisory activities on the basis of risk assessment of the OEs by the supervisors.

Weighting and Conclusion

The following deficiencies exist: (i) beneficial ownership threshold regarding entry controls for casinos and gambling operators is higher than permitted by the Standard and entry controls checks do not cover criminal associations (c. 28.1b); (ii) no market entry controls with a view to prevent criminals from entering the market exist for real estate agents and TCSPs, and very limited controls for accountants/auditors (c. 28.4); (iii) entry controls do not include criminal association or impose conditions regarding the ownership, control or management in DNFBPs other than casinos/gambling operators (c. 28.4); (iv) regulatory processes regarding risk-based supervision of DNFBPs by FID-SANS are under development thus compliance with c.28.5 cannot be demonstrated. **R. 28 is rated PC.**

Recommendation 29 - Financial intelligence units

In the 2013 MER, Bulgaria was rated C with the old R. 26.

Criterion 29.1 – The Financial Intelligence Unit of the Republic of Bulgaria, i.e., the Financial Intelligence Directorate of State Agency for National Security (FID-SANS) is established by the Law on State Agency for National Security (LSANS). The powers, functions and duties of the FIU are stipulated in several laws and regulations, including the Rules on Implementation of LSANS (RILSANS), the LMML, as well as the LMFT. FID-SANS is an administrative-type FIU.

In accordance with the RILSANS, the FID-SANS shall receive, store, examine, analyse and disclose information collected pursuant to the terms and order specified in the LMML, the LMFT and the LSANS and exercise control over the implementation of LMML, LMFT and the acts on their implementation. Besides its functions for receipt, storage, gathering, analysis and dissemination of financial intelligence and other relevant information, the FID-SANS is also one of the AML/CFT supervisors over the activities of the OEs under the LMML.

Criterion 29.2 – The general provisions of disclosing information on money laundering and/or financing of terrorism are regulated in the RILSANS, namely, Art. 32e.

(a) In accordance with Art. 32e (1) of the RILSANS, the FID-SANS shall receive, store, examine, analyse and disclose information collected pursuant to the LMML, LMFT and LSANS. According to Art. 32 (4) in execution of its obligations the FID-SANS shall receive notifications pursuant to Art. 72 of the LMML and Art. 9, Para 3 of the LMFT.

Art. 72 of the LMML provides that whenever there is a suspicion and/or knowledge of money laundering and/or that the proceeds of criminal activity are involved, OEs shall be obliged to notify immediately the FID-SANS. Art. 9, Para 3 of the LMFT stipulates analogue provisions in cases whenever suspecting and/or knowing of terrorist financing. However, there is a separate parallel reporting system for everyone who has knowledge of TF to Chairperson of SANS and MoI (Art. 9(1) of the LMFT). Neither the LMML nor LMFT cover explicitly the circumstances where there are reasonable grounds to suspect. However, this is considered as a minor deficiency since authorities presented to the AT the cases demonstrating that in practice this is done.

(b) According to Art. 76 of the LMML, OEs shall notify the FID-SANS of any payment in cash in an amount exceeding BGN 30000 or the equivalent thereof in a foreign currency made or received by a customer of the said persons in the course of the established relationship or in occasional transactions or operations.

The Bulgarian legislation appears to limit any kind of threshold-declarations to being cash-based. No other kind of information is required to be submitted pro-actively by the OEs, e.g., information on cross-border or national level payments.

Additionally to information submitted by the OEs, in accordance with Art. 77 of the LMML, the National Customs Agency (NCA) shall provide the FID-SANS with the information gathered by the NCA under the terms and according to the procedure established by the Foreign Exchange Act about any export and import trade credit, about financial leasing between residents and non-residents and about the carrying across the border of cash, precious metals and precious stones and articles made therewith or therefrom; and in accordance with Art. 78 thereof, Central Depository AD shall provide the FID-SANS with information about the issuing and disposition of dematerialised financial instruments under specified criteria.

Criterion 29.3

(a) The FID-SANS has the power to request information from OEs. The mentioned powers are mainly set out in Art. 74 of the LMML and Art. 9 of the LMFT.

(b) The FID-SANS has the possibility to request a wide range of information, including administrative and law enforcement information, from State and municipal authorities and such requests cannot be refused (see Art. 74 (4) of the LMML). Additionally, FID-SANS has the access to a range of information held by the BNB (Art. 74(8) and (9) of the LMML, Art. 9(3) and (6) of the LMFT), information held registries supported by state or municipal authorities (Art. 74(10) of the LMML, Art. 9(3) and (6) of the LMFT), information provided by supervisory authorities (Art. 87(1) of the LMML and Art.9a (2) of the LMFT), information submitted by the National Customs Agency and central depository (Art. 77 of the LMML and Art. 32e(7), item 1 of the RILSANS).

Additionally, the FID-SANS has the possibility to directly access a wide range of financial and administrative information, as well as law enforcement information, including, but not limited to: bank accounts and safe deposit boxes register, company/NPO register (incl. BO register), real estate register, social security and health insurance database (employment), tax authority (primary information), population register, register of criminal records, registry of wanted persons, Motor vehicle register, border control database.

Criterion 29.4 – The FID-SANS carries out analysis of information collected pursuant to LMML, LMFT and LSANS (see Criterion 29.2.), as well as other kinds of information received from OEs and/or state or municipal authorities.

(a) (*Met*) In accordance with Art. 32e(7), items 3-6 and (8) of the RILSANS, FID-SANS shall carry out financial intelligence analysis of operative files under LMML, collect additional information under the terms and according to the procedure established by Art. 74 of LMML, and draw conclusion whether the initial suspicion of money laundering is not dispelled. Operational analysis is performed in cases, where information on suspicion of ML/TF is filed by the OEs and/or state authorities, in cases where such information is received from international information exchange channels, as well as in cases of when "data mining" is performed and suspicion of money laundering or terrorism financing is identified.

(b) (*Met*) In accordance with Art. 32e(7), item 10 of the RILSANS, the FID-SANS shall carry out strategic analyses focused on the tendencies and schemes for money laundering and terrorist financing, on the basis of the information received under the terms and according to the procedure established by the LMML, LMFT and LSANS.

Criterion 29.5 – FID-SANS is able to disseminate, spontaneously and/or upon request with the relevant competent authorities.

Where, in the course of examining and analysing the information obtained under the terms and according to the procedure established by the LMML and/or the LMFT, the suspicion of ML and/or associated predicate offences and/or TF is not dismissed, the FID-SANS shall disseminate this information to the PO, to the relevant security service or public order service or to the competent specialised directorate of the SANS within their respective competence, as well as to the directorate referred to in Art. 16 (2) of the LCCIAF (see Art. 75(1) of the LMML and Art. 9b(1) of the LMFT).

Additionally, the FID-SANS shall respond to reasoned requests for the provision of information to the relevant security service or public order service, to the competent specialised directorate of the SANS or to the directorate referred to in Art. 16 (2) of the LCCIAF, where the said requests are based on suspicions of money laundering or associated predicate offences and/or financing of terrorism (Art. 75(2) of the LMML and Art. 9b(2) of the LMFT).

In regard to information exchange with supervisory authorities, in accordance with Art. 87(2) of the LMML and Art. 9a(3) of the LMFT FID-SANS and the supervisory authorities may exchange information for the purposes of the statutory functions performed thereby.

As to the usage of dedicated, secure and protected information dissemination channels, in accordance with the provisions of the LMML and the LMFT, information may be disseminated over protected channels of electronic communication subject to the requirements of the Classified Information Protection Act. Usually, the disclosures are conducted on paper. The correspondence of FID-SANS is always and only channelled through its own separate registrar's office (Art. 32e(3) of the RILSANS).

Criterion 29.6

(a) FID-SANS shall receive, store, examine, analyse and disclose information collected pursuant to the terms and order specified in the LMML, LMFT and LSANS (Art. 32e(1) of the RILSANS). The FID-SANS has a separate registrar's office and archive as well as a round seal and it shall establish, use, control and store its own database (Art. 32e(3) and (5) of the RILSANS).

The electronic data pool (FID-SANS' databases) is accessible only to FID-SANS employees conducting analysis and supporting the databases and handling the information is regulated either by Law on Protection of Classified Information or LMML.

When the documents contain information classified pursuant to the Law on Protection of Classified Information, all the rules for handling such information are applied, incl. the need-to know principle and the requirement for clearance for access to such information for the recipient's officials. When the documents do not contain information classified as State secret pursuant to the Law on Protection of Classified Information, the information is marked as protected under the LMML and the limitations under Art. 81 of the LMML are applied. Additionally, Art. 253b of the Criminal Code provides criminal liability for violation of the LMML by officials.

Although, the country has explained the procedure and rules for handling, storage, dissemination and protection of information, document setting out these rules was not provided to the assessment team due to confidentiality reasons (the relevant documents are classified pursuant to the Law on Protection of Classified Information). However, during the onsite the AT was able to verify the above-mentioned measures.

(b) A pre-condition for employing at FID-SANS is received the clearance for access to information Top Secret under the Law on Protection of Classified Information.

The employees of the FID-SANS shall not reveal, use for their own benefit or for the benefit of any persons closely linked therewith, any information and facts constituting an official, banking, trade or professional secret, as well as any other information and facts which the said employees have acquired in the performance of the official duties thereof. The employees hereof shall sign a declaration pledging to safeguard the respective secrecy (Art. 82 of the LMML).

(c) The electronic data pool (FID-SANS' databases) is accessible only to FID-SANS employees conducting analysis and supporting the databases and handling the information is regulated either by Law on Protection of Classified Information or LMML. There appear to be clear rules in place for the access of such data, however, the internal document governing these processes is classified and state secret and was not provided by the country. FID-SANS is located in premises with extensive security standards – both physical and IT wise.

FID-SANS premises can be accessed only by its employees. No other employees of SANS or other persons can access the premises of the FID and there are appropriate measures in place to ensure that there is limited access to FIU facilities and information, including information technology systems.

Criterion 29.7

(a) The FID-SANS is established by the LSANS. FID-SANS is an administrative type FIU. In accordance with Art. 32e of the RILSANS, the FID-SANS has the authority and powers to carry out its functions, mainly set out in the LMML and LMFT, freely, including, to receive, analyse and disseminate information. FID-SANS is represented by its Director, whose powers are mainly set out in Art. 32e (9) of RILSANS as well as other laws, e.g., LMML, LMFT, RILMML.

(b) FID-SANS is empowered to exchange information with the security services and public order services, the competent specialised directorates of the SANS within their respective competence, and with the Prosecutor's Office, under the terms and order established by LMML and LMFT (Art. 32e(7) of the RILSANS and Art. 75(2) of the LMML and Art. 9b(2) of the LMFT). FID-SANS and the supervisory authorities may exchange information for the purposes of the statutory functions performed thereby in accordance with Art. 87(2) of LMML and Art. 9a(3) of the LMFT. Additionally, FID-SANS can exchange information with its international counterparts in accordance with Art. 90(4) of the LMML.

(c) The core functions of the FID-SANS are embodied in Art. 32e(1) of the RILSANS (also refer to Art. 32e(2), (7) and (9) of the RILSANS. Art. 32e(6) of the RILSANS provides that other structural bodies of the SANS shall receive access to the data pool of the FID-SANS when cooperation is needed for prevention of encroachments against national security connected with financing of international terrorism and extremism or with money laundering and associated predicate offences therefore labelling other structures of the SANS in the same category as other state agencies.

(d) There are some minor issues that can affect the autonomy of FID-SANS. The FID-SANS is a part of SANS and there are some decisions and/or procedures that can be made or carried out only with the approval (signature) of the Chairperson of SANS (e.g., on-boarding of new employees require the signature of the Chairperson of SANS). As explained by the authorities, there have not been any cases where this would be an identified as an obstacle. Additionally, the AT has concerns regarding the budget allocation to FID-SANS. As the FID-SANS is part of the SANS, the budgetary allocations are assigned to the SANS and further distributed to directorates thereof. Although, the country has explained that there have been no complications within the assignment process, the lack of technical and human resources identified under Effectiveness Assessment leaves room for concerns.

Criterion 29.8 – The FID-SANS, in its capacity of Bulgarian FIU, has been a member of the Egmont Group since 1999.

Weighting and Conclusion

Art. 72 of the LMML provides that whenever there is a suspicion and/or knowledge of money laundering and/or that the proceeds of criminal activity are involved, OEs shall be obliged to notify immediately the FID-SANS. Art. 9, Para 3 of the LMFT stipulates analogue provisions in cases whenever suspecting and/or knowing of terrorist financing. However, there is a separate parallel reporting system for everyone who has knowledge of TF to Chairperson of SANS and MoI (Art. 9(1) of the LMFT). Neither the LMML nor LMFT cover explicitly the circumstances where there are reasonable grounds to suspect. However, this is considered as a minor deficiency since authorities presented to the AT the cases demonstrating that in practice this is done. (c.29.2(a)). There are also minor issues that can affect the autonomy of FID-SANS. The FID-SANS is a part of SANS and there are some decisions and/or procedures that can be made or carried out only with the approval (signature) of the Chairperson of SANS (e.g., on-boarding of new employees require the signature of the Chairperson of SANS). As explained by the authorities, there have not been any cases where this would be an identified as an obstacle. Additionally, the assessment team has concerns regarding the budget allocation to FID-SANS (c.29.7(d)). **R.29 is rated LC**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Bulgaria was not assessed for former Recommendation 27 as in the 3rd round it was rated LC. The reserve pertained to the effectiveness of money laundering investigations.

Criterion 30.1 – In the pre-investigative phase of the proceedings, the gathering of relevant information related to ML is mainly carried out by the relevant units of the two main General Directorates of the MoI (Police) that is, the Sector for Combating Crimes against Financial-credit System and Cybercrime within the Economic Police Department of the GD-NP, and the Sector of ML in the Department of Corruption and ML within the GD-COC. Also in the pre-investigative

phase, ML cases are dealt with the FSD-SANS as well. Preliminary inspection of TF cases is performed by the Specialized Directorate "Terrorism" of SANS.

The formal investigation of ML/TF offences and predicate offences is carried out by a system of authorities as pre-trial bodies (Art.193 of the CCP) interacting through an established mechanism where guidance and monitoring is provided by the prosecutor while the performance of specific investigative actions by investigators of the respective prosecutorial body or investigative police officers of the MoI.

In this context, ML offences are within subject to the jurisdiction of the district prosecutor's offices unless the Specialized Prosecutor's Office (SPO) has competence (in cases where ML was committed by an OCG). The actual investigation is carried out by investigators of the district POs or, if the case falls under SPO competence, the Investigative Department of the SPO as well as by investigative police officers of the MoI (from either GD or from territorial MoI bodies also). The National Investigation Service can investigate ML cases of factual and legal complexity except those under the competence of the SPO.

TF offences are in the exclusive competence of the SPO and is thus investigated by the Investigative Department of the SPO.

Criterion 30.2 – The examination of the property status of the perpetrator of a predicate offence is part of the investigative measures routinely aimed at identifying criminal proceeds (Art. 102 CCP) and the pre-trial bodies are empowered to investigate it within the pre-trial proceedings. The prosecutor investigating the predicate offence may continue to investigate ML in the same proceedings or in a separate case, if it remains in the competence of the same PO. If, however, suspicion of a related ML offence is established by a regional PO (which has no competence for such a crime) the case must be referred (either separately or together with the predicate offense) to the competent district PO or the SPO (or, in case of a related TF offence, exclusively to the SPO). As far as the investigative bodies are concerned, investigation officers of the MoI can be authorised by the competent prosecutor to pursue the investigation of any related ML/TF offences.

Criterion 30.3 – All LEAs and POs mentioned above are empowered to identify, trace, and initiate freezing and seizing of property subject to confiscation, including virtual assets, as part of their competences, although there is no legislation or mandatory instructions being in place to prescribe when and how such measures are to be carried out (e.g., in a parallel financial investigation) and neither is there any rule to provide for the expeditiousness of this procedure, apart from some the narrow and strict deadlines in the CPC (see under IO.8).

In the civil confiscation regime, the designated competent authority to meet C.30.3 is the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Commission (CACIAF), a state body established by the LCCIAF (a similar body had existed beforehand, established by preceding legislation from 2012). In this regime, assets acquired unlawfully (i.e. without a legitimate source) are subject to civil forfeiture, without prejudice to steps and measures taken under other laws, including the commencement of a criminal proceeding. One reason for instituting an unlawfully acquired assets forfeiture proceeding is that particular assets have been acquired by a person accused or suspected of any of the proceeds-generating criminal offences listed in Art. 108 of the said law (including ML and TF).

A CACIAF examination to identify and trace unlawfully acquired property will in such cases be triggered by a notification from the prosecutor supervising the respective case. The examination

is carried out by the competent territorial directorate of the CACIAF and its inspectors. As a result, the CACIAF has the powers to initiate the securing of such property and, eventually, to bring an action for the forfeiture of unlawfully acquired assets before the competent district court. (For further details see under R.4).

While the mechanism for identifying unlawfully acquired assets is thorough and detailed, it cannot be considered "*expeditious*" either. The procedure cannot be initiated until the acquirer of the property has already been accused or at least clearly suspected of a proceeds-generating criminal offence in a parallel criminal procedure. This is when the examination can be instituted and then the competent CACIAF directorate has a maximum 1 ½ year timeframe to examine and identify unlawful assets acquired by the respective individual, also including virtual assets, in the preceding 10 years.

Criterion 30.4 *(N/A)* – There are no such authorities in Bulgaria.

Criterion 30.5 – There are no investigative bodies in Bulgaria with a competence restricted to corruption crimes only. All bodies that investigate, among others, corruption offences have the power to identify, trace, and initiate freezing and seizing of assets in the scope of pre-trial proceedings. The aforementioned CACIAF is an anti-corruption authority but has no powers to investigate criminal offences (including ML/TF offences arising from, or related to, corruption).

Weighting and Conclusion

The mechanism available for identifying and tracing property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime by the CACIAF cannot be considered expeditious as required by C.30.3. **R.30 is rated LC**.

Recommendation 31 - Powers of law enforcement and investigative authorities

Criterion 31.1

(a) As noted above, Art. 159 CPC prescribes that in a formal investigation, all institutions, legal persons (including VASPs to the extent they are covered by legislation) as well as officials and citizens are obliged to preserve and hand over, upon request of the court or the pre-trial authorities, all objects, papers, computerized data and other data to the said authorities that may be of significance to the case.

Having said that, not all pre-trial bodies are equal in this, as production of documents in certain cases requires the action of the prosecutor. Specifically, only a prosecutor or a judge may require documents from a notary (see in the Law on Notaries and Notarial Activity) from a private enforcement agent (see in the Law on Private Bailiffs) and only prosecutors have access to the register of banking institutions, through individual, pre-determined employees to the Criminal Record Bureau, the Unified Portal of the Registry Agency, Population Register. The prosecutor is authorised to obtain a court decision for the disclosure of data and documents protected by secrecy (see Art 62 [6] of the Law on Credit Institutions) or that of data representing tax and insurance information in a criminal procedure (see the Tax and Social Security Code Art. 75).

(b) Rules governing the search of persons and premises in the formal investigative phase are provided under Art. 160 to 164 of the CCP in compliance with the respective FATF standards.

(c) Competent pre-trial authorities are empowered to take witness statements in the phase of formal investigation pursuant to Art. 117 to 124 and Art. 139 to 143 of the CCP.

(d) The CCP provides for detailed measures in this respect under Art. 159 (obligation to hand over objects, papers, computerised data) Art. 160 to 164 (search and seizure) and Art. 165 (interception and seizure of correspondence – not a SIM) applicable in the framework of a formal investigation.

Criterion 31.2 – Pursuant to Art. 172 (1) of the CPC, pre-trial bodies (the investigative authorities and the prosecutor) are authorised to use various SIMs including technical means (electronic and mechanical devices and substances that serve to document operations of the controlled persons and sites) and operational techniques (observation, interception, shadowing, penetration, marking and verification of correspondence and computerised information, controlled delivery, trusted transaction and investigation through an undercover officer) to obtain evidence in criminal proceedings. SIMs can be used for the investigation of a range of serious intentional criminal offences mentioned in Art. 172 (2) of the CPC including the ML offence (directly) and the TF offence (as part of Chapter 1 of the CC) if the relevant circumstances could not be established otherwise or only with exceptional difficulties. Detailed rules on the application of SIMs (both in the pre-investigative and the pre-trial proceedings) are provided by the Law on SIMs.

(a) Undercover operations are clearly covered by Art. 172 of the CPC (e.g., trusted transaction or deployment of an undercover officer) read together with Art. 10b and 10c of the Law on SIMs.

(b) Interception of communication is covered by Art. 172 of the CPC (interception of correspondence and computerised information) with further provisions in Art. 6 of the Law on SIMs (specifying that tapping by acoustic, technical, or other means shall be used to intercept oral, telephonic, or electronic communications of monitored persons).

(c) Accessing computer systems is covered by Art. 172 of the CPC (penetration of computerised information) with further provisions in Art. 8 of the Law on SIMs (specifying that this measure shall be used to ascertain by technical devices the presence of actual data on the premises or in articles used by monitored persons).

(d) Controlled delivery is clearly covered by Art. 172 of the CPC read together with Art. 10a of the Law on SIMs. This measure is applicable to the transportation "of an object, which makes the object of a criminal offence" which term is broad enough to encompass anything that is being smuggled or trafficked including cash or BNI having been or to be laundered.

Criterion 31.3

(a) An amendment to the Law on Credit Institutions in 2015 (in effect from 01.01.2017) established a special register (an electronic information system) of bank accounts kept and maintained by the BNB, containing information on the numbers of bank and payment accounts maintained by banks, payment institutions and electronic money companies, the title holders of accounts as well as authorised persons and BOs, and also on persons leasing safe-deposit boxes in banks and their attorneys (see Art. 56a of the said Law).

In the pre-investigative phase, the SD of SANS as well as MoI bodies have full electronic 24/7 access to this register which allows for rapid and accurate identification of accounts and also gives an opportunity to identify persons who manage or exercise control over these accounts. In the formal investigative phase, the bodies of the pre-trial proceedings also have direct access to the register by virtue of Ordinance RD-02-05/07.03.2017 of the Prosecutor General.

(b) The SD of SANS and the MoI Directorates have direct and online access, in the pre-investigative phase of the proceedings, to the electronic register of the Commercial Agency as well

as national registers of property including that of vehicles, vessels and aircrafts. In the phase of formal investigation, the prosecutor is authorised to request a court order for the disclosure of balances on bank accounts (see Art 62 of the Law on Credit Institutions) without the knowledge of the account holder. As for any other relevant information, Art. 159 CCP provides that upon request of the pre-trial authorities, all institutions, legal persons, officials and citizens are obliged to preserve and hand over all objects, papers, computerized data and other data, that may be of relevant for the case (including any registers and databases mentioned above). No such query involves the prior notification of the natural or legal person involved (see further details under c.4.2.a).

Criterion 31.4 – In the pre-investigative phase of the proceedings, the relevant security service or public order service, the competent SD of the SANS or the directorate referred to in Art. 16 (2) of the LCCIAF are authorized to request information from the FID-SANS in relation to suspicion of ML, associated predicate offences and TF pursuant to Art. 75 (2) of the LMML and Art. 9b (2) of the LMFT. In the formal investigative phase, the pre-trial bodies are empowered to request relevant information from FID-SANS pursuant to Art. 159 CPC which they can use as a basis for conducting investigative actions for gathering evidence.

Weighting and Conclusion

R.31 is rated C.

Recommendation 32 – Cash Couriers

Bulgaria was rated LC with the old FATF SR.IX. Apart from certain issues of effectiveness, the sole technical downgrading factor was the lack of power to restrain assets in case of ML or TF suspicions.

Criterion 32.1 – For incoming and outgoing cross-border transportation of cash and BNIs, Bulgaria has established a dual regime, with a declaration system applied at the external borders of the EU, and a disclosure system for the intra-EU movements of cash and BNIs. During the greatest part of the period subject to assessment, as at the time of the 4th round of MONEYVAL evaluations, the declaration regime was based on the EU Regulation (EC) 1889/2005 which was directly applicable in Bulgaria as an EU Member State, but its provisions were transposed and underpinned by the provisions of the Currency Act of 1999 (as amended) and Ordinance H 1 (01.02.2012) of the Minister of Finance on carrying across the border of the country of cash, precious metals, gems and items containing them or made of them and keeping the Customs register according to Art. 10 of the Currency Act.

Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (hereinafter: 2018 EU Regulation) entered in force on 3 June 2021 and has since been directly applicable. However, no amendments in national legislation to harmonize it with the new EU provisions were adopted by the end of the onsite visit, at which time only the domestic legislation transposing the previous (and already repealed) 2005 EU Regulation were in force in Bulgaria.

As far as the declaration/disclosure regimes are concerned, however, these are covered to an appropriate extent and provided for in sufficient details by the domestic legislation mentioned above and hence the failure to transpose the 2018 EU Regulation in time did not have any particular impact on the compliance with c.32.1 as well as c.32.2 and c.32.3 (as opposed to c.32.8).

With regards to the cross-border transportation of cash/BNIs via mail or cargo, Art. 11(2) of the Currency Act provides that no transfer of cash by post parcels is allowed unless with the indication of the declared value, in which case the respective regimes for declaration or disclosure apply (depending on which the other country is.)

It needs to note that, as far as external borders of the EU are concerned, the 2018 EU Regulation (EU) clearly provides for controls of cash/NBIs sent by post, freight, or courier shipment. If the cash is to be sent in postal packages, courier shipments, unaccompanied luggage, or containerized cargo ("unaccompanied cash"), the competent authorities have the power to request the sender or the recipient to make a declaration. Competent authorities have the power to carry out controls on any consignments, receptacles or means of transport which may contain unaccompanied cash. In lack of the necessary amendments to the Currency Act, however, these provisions of the 2018 EU Regulation were not in effect (even though being in force) at the time of the onsite visit.

Criterion 32.2 – The declaration system at the EU external borders, as mentioned under c.32.1, obliges any natural person entering or leaving the territory of the EU carrying cash in amounts equal to or greater than EUR 10.000 by virtue of Art. 11a of the Currency Act (in line with the previous and the new EU Regulations, which also define that the term "cash" extends to BNIs in general). Passengers who meet this criterion are obliged to declare this fact in writing, by use of the declaration form prescribed by the aforementioned Ordinance H1 of 2012.

New declaration forms were introduced by Commission Implementing Regulation (EU) 2021/779 of 11 May 2021 (applicable as from 3 June 2021) establishing templates for certain forms as well as technical rules for the effective exchange of information under the 2018 EU Regulation.

Criterion 32.3 – The domestic disclosure system at the EU internal borders, similarly to the declaration regime mentioned under c.32.2, applies to any natural person crossing the border between Bulgaria and other EU Member States (i.e. Greece and Romania) while carrying cash or BNIs in amounts equal to or greater than EUR 10 000. In such cases, a cash declaration shall be submitted upon the request of the Customs authorities (Art. 11b of the Currency Act) using the declaration form mentioned above under c.32.2.

Criterion 32.4 – Art. 16 (1) of the Currency Act and Art. 15 (2) point 7 of the Customs Act provide that Customs authorities have competence to apply controls on cash movements across the state border. The powers of Customs authorities are defined in Section III of the Customs Act, where the power to require documents and further information (explanations) from persons subject to customs control is specifically provided under Art. 16 (1) particularly in points 1, 3, and 5.

Criterion 32.5 – As for the declaration regime applicable at EU external borders, failure to comply with the obligation under Art. 11a of the Currency Act by refusing to make a declaration or by providing deliberately incorrect or incomplete information therein (see Art. 11a [5]) is an administrative offence under Art. 18(2) of the same Act (also in line with the 2018 EU Regulation and its predecessor). It is punishable by a fine (for natural persons) or a pecuniary sanction (for legal entities and sole traders) in the amount of 1/5 (20%) of the value of the undeclared cash, precious metals, or gems. (In this context, BNIs are clearly covered by the definition of "cash" in §1 paragraphs 6-7 of the supplementary provisions of the Currency Act and, in relation to the regime applicable at EU external borders, also by the 2018 EU Regulation). In case the offence committed by concealing the respective cash or other valuables, the penalty is 1/4 (25%) of the value (see para [3]) while in case of repeated violation, the same penalties go up to 1/4 (25%) and 1/3 (33%), respectively (see para [7]). There is no absolute minimum or maximum penalty.

As for the disclosure regime at internal EU borders, Art. 11b (3) of the Currency Act provides quite similarly as above. Refusing to make a declaration upon request or providing deliberately incorrect or incomplete information is a separate administrative offence under Art. 18a (1) punishable by a fine of 1000 to 3000 BGN (€ 512 - €1 534) for natural persons or a pecuniary sanction of 2 000 to 6000 BGN (€ 1 023 - € 3 069) for legal entities and sole traders. The maximum amounts (around €1 500 and €3 000 respectively) do not seem to be dissuasive, even if in case of a repeated violation, the offender will be subject to a fine (or pecuniary sanction) in double amount than the previously imposed one.

Failure to comply with the obligation to declare at EU external borders pursuant to Art. 11a of the Currency Act constitutes a criminal offence under Art. 251 of the CC if the value of the object of the offence is of particularly large amount, that is, it exceeds 140 times the minimum working salary, as defined by the Supreme Court in its Interpretative decision № 1 dated 30.10.1998. At the time of the onsite visit, the minimum working salary was 650 BGN (€332)[115] and thus the "particularly large amount" above was €45 500. This crime is punishable by imprisonment for up to 5 years or by a fine in the amount of 1/5 (20%) of the value of the object of the crime. Considering that fine can be an individual punishment, one needs to note that the administrative offence may easily carry a more severe penalty than this (up to 33% of the value).

Furthermore, no similar criminal offence seems to exist for large-scale cases of failure to comply with the disclosure regime at EU internal borders. As it was explained by the authorities, failure to comply with the obligation to declare cash at EU internal borders (e.g., crossing the border without submitting a declaration on request of the Customs authorities) is an administrative offence, regardless of the amount transported, which makes the criminal sanctioning regime incomplete.

Criterion 32.6 – Information about declared cash/BNIs as well as any violations of the obligation to declare or disclose are stored in the Bulgarian Integrated Customs Information System and are made available to the FIU in accordance with Art. 77 of the LMML. Such information, however, is only submitted to the FIU monthly, pursuant to Art. 55 of the RILMML which is far from the direct availability required by this criterion.

As far as information derived from the functioning of the declaration regime at EU external borders is concerned, Art. 9 (3) of the 2018 EU Regulation provides that the competent authorities shall transmit this information as soon as possible, and in any event no later than 15 working days after the date on which the information was obtained. The technical rules for transmission by electronic means of the information are established by the Commission Implementing Regulation (EU) 2021/779 (see c.32.2). The exchange of information is carried out via the Customs Information System (CIS) established under Council Regulation (EC) 515/97 on mutual administrative assistance in customs matters. The FID-SANS may thus have access to information entered to CIS earlier than the one-month timeframe mentioned above, but only as regards data from the EU external borders are concerned.

This apparent deficiency is, however, remedied by Instruction No.I-7 of 26.10.2018 on the access of SANS to the databases of the National Customs Agency. This Instruction was issued by the heads of the two governmental bodies (and therefore it is rather a MoU than an instruction). It provides the SANS bodies (including the FIU) carrying out the activities assigned by law

[115] Council of Ministers Decree No 331/2020, promulgated SG 103/2020, in force from 01.01.2021.

(including the LMML) to the SANS, immediate and direct access to the automated information system of the NCA including data from cash declarations and/or those relating to any associated criminal offences.

Criterion 32.7 – Instructions for cooperation between Customs authorities and Ministry of Interior (MoI) as well as the National Revenue Agency (NRA) give the legal basis for information exchange and the access to the information systems for reference purposes in order to prevent and detect customs, currency and tax violations and crimes. Within this interaction, the NRA provides the Customs authorities with access to some of their electronic services and the MoI to their respective databases, while the Customs provide the said authorities with specific data from particular information systems including those about cash carried across the border of the country.

Criterion 32.8 – Art. 7 of the 2018 EU Regulation provides that the competent authorities may temporarily detain cash (including BNIs) where: (a) the obligation to declare or to disclose cash is not fulfilled or (b) there are indications that the cash, irrespective of the amount, is related to criminal activity (the preceding EU Regulation only provided for the first option).

Since the 2018 EU Regulation is directly applicable in Bulgaria, c.32.8 is formally met by the above provisions to the extent it concerns transport of cash through the external borders of the EU. On the other hand, even if the EU legislation applies without domestic implementation, there is need for appropriate national legislation to set out roles and responsibilities of domestic authorities in this field, together with the necessary procedural rules, otherwise it might be "in force" but not "in effect" in the given country. This could have been achieved by relevant amendments to the Currency Act and the amending legislation had indeed been prepared but, finally, was not adopted by the end of the onsite visit. As a result, the practical applicability of the 2018 EU Regulations was not provided for within the time period relevant for this assessment.

Furthermore, there is no legislation (having been adopted by the end of the onsite visit) to give power to the authorities to stop/restrain cash being transported across the EU internal borders (i.e. beyond the scope of the 2018 EU Regulation) unless there is a clear suspicion of the criminal origin of the respective assets which can give rise to the application of criminal procedural measures.

Criterion 32.9 – As far as information derived from the declaration mechanism applied at the external borders of the EU is concerned, the general requirement for exchange of information among EU countries is regulated by Art. 10 of the 2018 EU Regulation (Art. 6 of the previous EU Regulation 1889/2005) (technical rules for transmission are the same as discussed above under c.32.6). As a main rule, such information shall be transmitted as soon as possible, but no later than 15 working days from its obtainment.

The exchange of such information with third countries is based on Art. 11 of the 2018 EU Regulation (Art. 7 of the previous Regulation) and may take place within the framework of mutual administrative assistance, subject to the written authorization of the competent authority which originally obtained the information and in compliance with the relevant national and EU law on the transfer of personal data to third countries. The Naples II Convention as well as bilateral and multilateral agreements provide further basis for international customs cooperation in non-EU relations and the same are used for exchanging of information derived from the disclosure regime applied at EU internal borders. In the course of criminal proceedings, MLA may be sought and provided (see R.37-38).

The retention period for cash declarations generally is 5 years pursuant to Art. 10a of the Currency Act. In addition, Art. 13 of the 2018 EU Regulation also requires that the customs authorities and the FIU store personal data obtained through the operation of the declaration regime at the external borders of the EU for a period of 5 years (which may be extended by 3 more years under specific conditions). Information on cross-border transport of cash or BNIs that has been provided to FID-SANS under Art. 77 of the LMML is retained in the databases of the recipient authority for 10 years according to Art. 70 of the LMML.

Criterion 32.10 – Bulgaria, as an EU Member State, applies the safeguards to the personal data privacy ensured by Art. 12 of the 2018 EU Regulation (Art. 8 of the previous EU Regulation 1889/2005) which are underpinned, also with regard to data derived from the disclosure regime applied at EU internal borders by Art. 10a (5) of the Currency Act and Art. 17a of the Customs Act, all providing for strict safeguards and proper use of the information collected through the declaration / disclosure systems. EU Regulation 45/2001 on the data protection is also directly applicable in this context to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

Criterion 32.11 – Natural persons transporting cash or BNI related to ML/TF or predicate offences are subject to the same criminal sanctions as referred under R.3 and R.5 above, in which case the general confiscation and provisional measures regime would be applicable to the respective currency or BNIs.

Weighting and Conclusion

The criminal sanctioning regime is incomplete as it only exists for large-scale cases of non-compliance at the external EU borders. Temporarily retainment of cash in the sense of c.32.8 is only formally provided at the EU external borders, but domestic legislation for the practical application of this mechanism is still not in place, while there is no such mechanism at all for the EU internal borders, as a result of which there are currently no legal powers for the detention of cash suspected to be linked to ML/TF. **R.32 is rated PC.**

Recommendation 33 – Statistics

In its 2013 MER, Bulgaria was rated LC with the old R.32. The MER identified the following deficiencies: The Interagency council for monitoring National Strategy, review the system, and coordination of the system as a whole not yet created; the review of results and outputs of the AML/CFT systems (and the effectiveness of the systems as a whole) is not a regular and systematic process; FSC is encouraged to keep statistics on the scope of international requests to identify AML/CFT requests. Considering that R.32 was rated LC in the 4th round MER, Bulgaria has not informed of any developments in the course of the 4th round follow-up process.

Criterion 33.1 *(Partly Met)* – Bulgarian law provides that the country shall keep statistics only "For the purpose of conducting an NRA". In accordance with Art. 71(1) of the LMML competent authorities shall maintain statistics on matters relevant to the effectiveness of the systems to prevent and combat ML/TF. There are no requirements set out in law (nor internal guidelines) that would require competent authorities to maintain comprehensive statistics relevant for the effectiveness and efficiently of the country's AML/CFT system. Despite the technical requirements set out below, the Effectiveness Assessment has revealed that the level of statistics kept is insufficient.

(a) (*Partly met*) *STRs received and disseminated* - In accordance with Art. 71(2) item 3 of the LMML statistics include data assessing the stages of reporting of cases of ML/TF. There are major concerns regarding the level of breakdown of the statistics kept – although number of STRs received is maintained by the country, there is no breakdown of predicate offences listed in the STRs, STRs used in disseminations, and other metrics that would allow for assessment thereof.

(b) *(Partly met) ML/TF Investigations, Prosecutions and Convictions* – pursuant to Art. 71(2) item 2 of the LMML, statistical data shall also include data measuring the pre-investigation, investigation and judicial phases of cases of ML/TF. In particular, these statistics must include: the number of checks conducted by the LEAs on an annual basis; the number of cases investigated on an annual basis; the number of persons against whom criminal proceedings are instituted; the number of persons convicted for money laundering or financing of terrorism; the types of predicate offences. However, Bulgarian authorities could only provide very general statistics.

(c) (*Partly met*) *Property frozen, seized and confiscated* – pursuant to Art. 71(2) item 2 of the LMML, statistical data on the value of property that has been frozen, seized or confiscated, calculated in Lev or equivalent shall be gathered by the relevant competent authorities. However, Bulgarian authorities could only provide very general statistics. There is no statistics on breakdown by predicate offences where assets are seized or confiscated.

(d) (*Partly met) MLA or other international requests for co-operation made and received* – pursuant to Art. 71(2) item 5 of the LMML, the FID-SANS shall maintain data regarding the number of cross-border requests for information that have been made, received, refused and partially or fully answered. Such information shall be grouped by countries. Other competent authorities according to item 6 of Art. 71(2) of the LMML shall maintain data regarding the number of cross-border requests for information that were made, received, refused and partially or fully answered. Notwithstanding the mentioned, the country only keeps the minimum level of statistics, which affects the quality of any analysis related to international crimes.

Weighting and Conclusion

Although legal requirements to comply with c.33.1 are in place, the country only keeps a minimum level of statistics on (a) STRs received and disseminated (b) ML/TF investigations, prosecutions and convictions, (c) property frozen, seized and confiscate, (d) MLA or other international requests for co-cooperation made and received. Additionally, gathering data is a major manual work for the country. Therefore, the AT cannot conclude that Bulgaria maintains comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system. The country is encouraged to keep more detailed statistics. **R.33 is rated PC.**

Recommendation 34 – Guidance and feedback

In the 2013 MER, Bulgaria was rated LC on former R. 25. The AT has identified the following shortcomings: (i) some OEs demonstrated little awareness of the available methodological guidelines; (ii) many of the guidelines appeared to be generic and not tailored to the particular sector (efficiency issue); (iii) limited specific feedback provided to non-banking OEs; (iv) limited awareness raising initiatives for DNFBP sector on ML/TF typologies and guidance.

Criterion 34.1

Legal basis

In respect of Guidelines and feedback in applying national AML/CFT measures, Art. 32(e)(7)(21) of the RILSANS provides for general outreach activities of the FID-SANS to OEs; Art. 32e(7)(22) of the RILSANS provides for methodological assistance of the FID-SANS to OEs; Art. 32e(7)(29)

provides for the publishing of the annual report of the FID-SANS in its capacity of FIU, which contains both kind of summarized feedback and general guidance on AML/CFT issues.

The BNB also has a legal basis for issuing guidance regarding corporate governance of banks under Art. 73(4) of the LCI which includes systems for ML prevention; as well as guidance stemming from the guidelines, recommendations and other measures of the EBA which also might include AML/CFT matters.

Guidance issued

FID-SANS published various guidance documents on its website, including the application of AML/CFT measures (covering ML and to a lesser extent TF and TFS), changes to AML/CFT laws, identifying and reporting suspicious transactions, and treatment of NPOs. All published documents are generic, do not cover the possible *red flags, risk factors* and *typologies* relevant to different supervised sectors and do not discuss any vulnerabilities of broad range of products and services that fall under AML/CFT legislation.

In 2016 and 2017 FID-SANS issued very specific guidance on red flags regarding TF financing activities and distributed it to banks. In 2021 FID-SANS issued three guidance documents regarding risk indicators for corruption (incl. PEPs), trade-based money laundering and complex corporate structures. Again, these were distributed only to banks. There is currently no guidance published by the BNB, the FSC, the NaRA or the CRC other than the provision of links to EU guidance on the website of the BNB and the FSC. However, the BNB has provided guidance directly to credit institutions under its supervision. This includes some general Guidance in 2009 and 2012 (relevant until March 2018 when the changes to LMML have been introduced) on filing requirements (although this is rather historic and does not address the significant changes introduced by Bulgaria to reflect the new AML regime specified in the LMML) as well as joint BNB and FID-SANS guidance on NPOs and PEPs in 2021.

A large number of European Supervisory Authorities (ESAs) guidance papers have been published that are applicable to larger or smaller extent to FIs in Bulgaria. On the basis of provisions of the LMML some provisions of the ESAs guidance are legally binding. Banks are legally required under Art. 74a LCI to comply with EBA guidelines and are subject to sanctions for non-compliance under Art. 103(1).

Outreach activities

Throughout the reporting period, FID-SANS has conducted or participated in a number of trainings for OEs and representative groups covering a large proportion of FIs and DNFBPs. To date, trainings appear to have been focused on changes to LMML/LMFT and application of measures as opposed to identification of risk factors and red flags. Individual meetings have been held regarding violations and STR quality, but no seminars were held in this regard. However, in 2020, 12 training sessions were held regarding the findings of the NRA. Some trainings were specifically held regarding application of BO requirements in response to violations identified through onsite supervision.

The BNB conducts regular meetings either independently or jointly with FID-SANS and the AML/CFT units of supervised entities. Experts also participate in workshops and seminars and the BNB-SSAD holds annual meetings with the Association of Banks in Bulgaria (which continued remotely during the Covid-19 pandemic) and issues circulars to supervised entities regarding

particular issues and topics including circulars to banks regarding bitcoins, binary options and fraud schemes (2014-16), Luanda leaks, UNSC resolutions, OFAC designations of Bulgarian persons (2021) and new EBA Risk Guidelines (2021). The BNB also provides guidance to OEs on an ad hoc basis when requested.

The FSC has provided AML/CFT trainings including joint training sessions with FID-SANS in 2016 and has established a platform whereby information and educational materials are uploaded and made available to OEs. The FSC also provides consultations to OEs on an ad hoc basis when requested and provides guidance and recommendations through its inspection process.

No outreach has been performed by either the NaRA or the CRC either independently or jointly with the FID-SANS.

Despite not being AML/CFT supervisors, both the Supreme Bar Council and the Notaries Chamber provide training and outreach for members. Lawyers are required to participate in annual trainings by the Supreme Bar Council which includes trainings on LMML requirements. The Notaries Chamber has provided a total of 15 training seminars with AML/CFT focus in 2018-2020.

Feedback

In respect of feedback on reporting suspicious transactions: Art. 72(4) of the LMML and Art. 9(7) of the LMFT states that the FID-SANS shall provide FIs and DNFBPs with feedback related to the filing of STRs. The FID-SANS has developed both a *Sample Template for STRs* (Art. 72(8) of the LMML and Art. 51 and 52 of the RILMML) and *Guidelines on STR submissions*[116]. The FID-SANS in its FIU capacity also produces an annual report on the activities of FID-SANs[117]. These reports contain short sections on ML trends and a few case studies, e.g., the report of 2019 contained 3 case studies; the report of 2018 – 4 case studies. All in all, very limited consolidated feedback is being provided by FID-SANS to the OEs to assist them in detecting and reporting suspicious transactions.

FID-SANS also publishes on its website list of the imposed sanctions for non-compliance including the relevant legal provisions that were breached.

Weighting and Conclusion

Moderate deficiencies exist: (i) FID-SANS published guidance is generic and not tailored to specific FI/DNFBP types; very limited consolidated feedback is being provided by FID-SANS to the OEs to assist them in detecting and reporting suspicious transactions; (ii) guidance on specific red flags has been provided only to banks, other sectors have not been covered; (iii) there is currently no guidance other than links to European Guidance published by the BNB, the FSC, the NaRA or the CRC; (iv) No outreach has been carried out by the NaRA or the CRC either independently or jointly with the FID-SANS. **R.34 is rated PC**.

Recommendation 35 – Sanctions

In the 2013 MER, Bulgaria was rated largely compliant with former R. 17. The AT found that maximum monetary fines for AML/CFT breaches were not dissuasive.

---

[116] http://www.dans.bg/en/msip-091209-menu-en/guidance-fr-060712-mitem-en;http://www.dans.bg/en/msip-091209-menu-en/sample-forms-adopted-by-the-director-of-fid-sans

[117] http://www.dans.bg/en/msip-091209-menu-en/fidannualreports30052012-mitem-en

Criterion 35.1 Bulgaria has a range of sanctions including criminal and administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT obligations as well as persons who tolerate the commission of violations.

Administrative financial penalties

Administrative penalties are provided in LMML and LMFT for cases where the act does not constitute a crime. Where the act does constitute a crime, the penalties within the Criminal Code apply. Administrative penalties are provided for in Chapter 10, particularly Articles 116 and 118 of the LMML regarding legal AML violations and Art. 15 of the LMFT regarding legal CFT and TFS related to TF violations, in both cases violations regarding STR reporting requirements and tipping-off are included. Range of penalties are discussed below.

Non-compliance with the STR reporting requirements under Art. 72 of the LMML and Art. 9(3) and (5) of the LMFT is punishable with the range of sanctions stipulated under Art. 116 and 117 of the LMML and Art. 15 of the LMFT (as per Art. 108(6) of the LMML, supervisors other than the FID-SANS do not have powers to supervise OEs with the STR reporting requirements regarding ML whereas all supervisors have necessary powers regarding TF under Art. 9A(2) of the LMFT). Non-compliance with the prohibition of tipping-off is punishable under Art. 80(1) of the LMML and Art. 9(13) of the LMFT, with the range of sanctions stipulated under Art. 116 and 117 of the LMML and Art. 15 of the LMFT.

FID-SANS has powers to sanction for all the above stipulated breaches. In addition, penalties may also be imposed by the BNB, the FSC and the NaRA (regarding gambling) under Art. 123(1) of the LMML and Art. 16(1) of the LMFT for the above stipulated breaches except LMML STR reporting requirements. In cases where joint supervision is conducted by the FID-SANS and the BNB, the FSC or the NaRA, sanctions are determined on the basis of Instructions for Joint Supervision (MoUs) with either party able to sanction.

Penalties range for natural persons from BGN 1 000 to BGN 10 000 (approx. € 500 to € 5 000) in LMML and BGN 2 000 to BGN 20 000 in LMFT (approx. € 1 000 to € 10 000); for legal persons and sole traders BGN 2 000 to BGN 20 000 (approx. € 1 000 to € 10 000) in LMML and BGN 20 000 to BGN 50 000 in LMFT (approx. € 10 000 to € 25 000); for financial institutions, except PMOs, BGN 5 000 to BGN 50 000 (approx. € 2 500 to € 25 000) in LMML and BGN 30 000 to BGN 100 000 in LMFT (approx. € 15 000 to € 50 000). For repeated violations these increase to up to BGN 20 000 (approx. € 10 000) for natural persons (same under LMFT), BGN 50 000 (approx. € 25 000) for legal persons and sole traders, BGN 100 000 in LMFT (approx. € 50 000) and BGN 200 000 (approx. € 100 000) for financial institutions, except PMOs (same in the LMFT). According to Art. 119 of the LMML and Art. 15(4) of the LMFT the penalties can be applied to persons who manage and represent an OE as well as those responsible for exercise on internal controls over compliance where they have allowed or participated in the commission of the violation.

Additionally, Art. 117(2) LMML and Art. 15(3) LMFT provide for more severe penalties in cases where there are serious or systemic violations. The values are the same in LMML and LMFT:

- for natural persons – up to BGN 2 000 000 (approx. €1 000 000);
- for legal persons and sole traders – up to BGN 2 000 000 (approx. €1 000 000); or up to the double amount of the benefit derived from the violation, if the said benefit can be identified;

- for financial institutions – BGN 10 000 000 (approx. €5 000 000), or up to 10 per cent of the annual turnover, including gross income according to the consolidated financial statement of the parent undertaking for the previous year, comprising interest receivable and other similar income, income from shares and other variable or fixed yield securities income and receivables from commissions and/or fees.

Criminal sanctions

Art. 253b of the Criminal Code establishes that any official who violates or fails to comply with the provisions of the LMML shall be punished, in cases of significant impact, with imprisonment for up to three years and a fine from BGN 1 000 to BGN 3 000 (approx. €500 to €1500), unless the deed does not constitute a more serious crime. The Criminal Code does not provide for penalties regarding such "more serious" crimes and Art. 253b does not extend to failure to comply with the LMFT requirements.

Regulatory sanctions

Art. 125 of the LMML permits the licensing or registration authority either on its own initiative or on proposal by FID-SANS to withdraw authorisations for licence or registration in cases of repeat violations (under the terms established at Art. 116(2)) or serious or systematic violations at Art. 116(3) of the LMML). Equivalent provisions are at Art. 15(8) of the LMFT.

Art. 126 of the LMML permits FID-SANS to order an OE to cease a violation and to take specific measures necessary for remedying the said violation, as well as set a time limit for the taking of such measures. The same applies regarding TF and TFS compliance under Art. 14a of the LMFT.

Art. 122(1) of the LMML provides for the possibility to publish information on administrative sanctions issued by the supervisory authorities to the OEs for violations of the LMML and RILMML. However, where the publication could be regarded as disproportionate measure or would jeopardise the stability of the financial markets or ongoing criminal proceedings, the FID-SANS and supervisory authorities are allowed to: (i) delay publication, (ii) made information public without disclosing personal data of individual or legal person upon which such a sanction have been imposed and/or (iii) not to make information on sanction public.

In addition, the BNB and the FSC have additional sanctioning powers to the ones discussed above with respect to banks, payment and e-money institutions and entities operating in the securities field.

(1) Regarding banks, the BNB may issue supervisory measures regarding violations of both the LMML and LMFT under Art. 103(1)(8) of the LCI. Measures include at Art. 103(2) issuing written warnings, convening of a meeting of shareholders or managing board to request adoption of resolution to change the specialised auditing entity, issuance of a written order to cease and desist violations, or issuance of written order to make AML/CFT improvements. The BNB also has powers to suspend or restrict the licence of a bank under Art. 103(2) LCI.

(2) Regarding payment institutions and e-money institutions, Art. 169(1) of the LPSPS lists the measures that may be taken by the BNB in respect of violations of both the LMML and LMFT as per Art. 173(9), including: written warning, order to discontinue and/or rectify breaches within a given time-limit, require changes in the internal rules and procedures, and forbid conducting of some or all activities until irregularities are resolved. Further measures are provided at the Art. 170(1) of the LPSPS, including requirement to carry out ad hoc audit,

imposition of additional supervisory requirements, prohibitions or restriction of volume of specified transactions, activities or operations, and withdrawal of licence. The BNB also has powers to suspend or restrict the licence of a payment institution or e-money institution under Articles 169(1) and 170(1) of the LPSPS.

(3) Regarding securities, the FSC may impose regulatory measures in respect of LMML violations under Art. 276(2) in relation to an investment firm, market operator or regulated market and under Art. 264(9) of the CISOUCIA in respect of a person who manages an AIM fund, collective investment scheme or other collective investment undertaking. In both cases this includes measures to compel remediation and issue a public warning under Art. 24(2)(c) of Regulation (EU) No. 1286/2014. The FSC may revoke authorisation of licence in cases where there are violations of LMML: of an investment firm (Art. 27(1)(9) of the MFIA), of a regulated market (Art. 166(1)(5) of the MFIA), of an investment company (Art. 19(1)(6) of the CISOUCIA), of a management company (Art. 100(1)(8) of the CISOUCIA), a national investment company (Art. 180(1)(6) of the CISOUCIA), an alternative investment fund manager having seat in a third country (Art. 212(1)(6) of the CISOUCIA). However following shortcomings still apply in relation to FSC: (1) provisions do allow for the FSC to restrict (as opposed to revoke) a licence; (2) sanctioning powers of the FSC do not extend to sanctions for non-compliance with LMFT; (3) no power to revoke licence of AIM regarding the LMML violations; (4) the list of reasons to revoke licence of an alternative fund manager at Art. 201(1)(6) of the CISOUCIA does not include violations of the LMML

(4) Regarding insurers, under Art 40(2)(4) of the Insurance Code, the FSC may revoke the licence of an insurer or reinsurer in cases where licence conditions are not complied with. It remains unclear whether LMML/LMFT compliance is stipulated as a licence condition. No further regulatory sanctions have been identified regarding insurers and reinsurers and none have been identified regarding social insurance (pensions), except for the general provision at Art. 125 of the LMML which permits supervisory authorities to revoke licence in cases of repeat or systemic violations.

The NaRA (regarding gambling) does not have any sanctioning powers other than the ability to impose financial penalties as described above; and the NaRA (regarding currency exchange) and the CRC (regarding postal operators) have no powers to sanction for non-compliance with either LMML or LMFT.

Overall, considering the maximum monetary values of fines applicable and criminal penalties it is possible to conclude that administrative and criminal sanctions are proportionate and dissuasive to a large extent, however, regulatory sanctions are not sufficient, particularly regarding violations of LMFT.

Targeted Financial Sanctions

Sanctions for TFS related to TF violations are provided under Art. 15 of the LMFT and these include: (1) a fine of BGN 2 000 (approx. € 1 000) or exceeding this amount but not exceeding BGN 10 000 (approx. € 5 000), where the offender is a natural person; (2) a pecuniary penalty of BGN 20 000 (approx. € 10 000) or exceeding this amount but not exceeding BGN 50 000 (approx. € 25 000), where the offender is a legal person or sole trader; (3) a pecuniary penalty of BGN 30 000 (approx. € 15 000) or exceeding this amount but not exceeding BGN 100 000 (approx. € 50 000) where the offender is an OE. Sanctions for non-compliance with the TFS related to TF requirements are not fully dissuasive, especially with respect to maximum amount of fine applicable to financial institutions (except PMOs).

No sanctions are available for non-compliance with TFS related to PF.

NPOs

See criterion 8.4(b).

Criterion 35.2 – Administrative sanctions applicable to directors and senior management are listed under Art. 117(1), Art. 119(1) and Art. 120(3) of the LMML and Art. 15(4) of the LMFT. Monetary penalties applicable to directors and senior management do not seem fully dissuasive: penalties range from BGN 1 000 to BGN 10 000 (approx. € 500 to € 5 000) in the LMML and BGN 2 000 to BGN 20 000 (approx. € 1 000 to € 10 000) in the LMFT. The provisions apply to any person who manages and represents an FI/DNFBP covered under the LMML. The sanctions also apply to any person who is responsible for the exercise or who exercises the internal control over compliance with the AML/CFT obligations of the entity, where the said persons have committed or have tolerated the commission or have participated in the commission of the violation.

In addition, persons that have been issued an administrative sanction for serious and repeated violations are prohibited from occupying a senior management role for a period of 3 months or 1 year (Art. 124(1) and 124(2) LMML and Art. 15(7) LMFT).

Targeted Financial Sanctions

Sanctions for TFS related to TF violations are provided under Art. 15 of the LMFT and these include a fine of BGN 2 000 (approx. € 1 000) or exceeding this amount but not exceeding BGN 10 000 (approx. € 5 000), where the offender is a natural person.

NPOs

See criterion 8.4(b).

Weighting and Conclusion

Moderate shortcomings exist: (i) Criminal Code does not provide for more dissuasive penalties for *more serious* crimes; (ii) Criminal Code applies only to the LMML violations and not to the LMFT violations; (iii) the FSC is not able to restrict (as opposed to revoke) a licence; (iv) the FSC is only able to revoke licence regarding the LMML violations and not for the LMFT violations, however, no powers to revoke a license of an AIM; (v) the FSC has no legal basis for issuing written warnings or orders to address violations; (vi) the NaRA (regarding gambling) has no legal basis to sanction other than imposition of administrative financial penalties; (vii) monetary penalties applicable to directors and senior management are not fully dissuasive; (viii) sanctions for non-compliance with the TFS related to TF requirements do not appear fully dissuasive, especially with respect to maximum amount of fine applicable to OEs; (ix) no sanctions are available for non-compliance with TFS related to PF. Consequently, **R.35 is rated PC.**

Recommendation 36 – International instruments

In the 2013 MER, Bulgaria was rated LC with the previous R. 35. The MER identified the following deficiencies: implementation of Vienna and Palermo Conventions are not fully observed; the TF offence is not fully compliant with the TF Convention; there are limitations for application of confiscation. Considering that R.35 was rated LC in the 4th round MER, Bulgaria has not informed of any developments in the course of the 4th round follow-up process.

Criterion 36.1 – Bulgaria is a party to the Vienna Convention (effective for the Republic of Bulgaria since 23.12.1992), the Palermo Convention (effective for Republic of Bulgaria since

29.09.2003), the Merida Convention (effective for the Republic of Bulgaria since 20.10.2006) and the Terrorist Financing Convention (effective for Republic of Bulgaria since 19.03.2001.).

Criterion 36.2

Vienna Convention – Bulgaria has implemented most of the provisions of the Vienna Convention. However, there are deficiencies with implementation of Art. 5, where the seizure and confiscation could not be extended to the instrumentalities used and intended for use in the commission of ML and TF and to the object of the crime in cases where the property is held by a third party, as well as legitimate property intermingled with the illegally obtained property. With regards to implementation of Art. 7, the shortcomings identified with respect to the provisional and confiscation measures may have a negative impact on MLA requests. Deficiencies identified in R. 3 and R.4 have an effect on the implementation of Vienna Convention by Bulgaria.

Palermo Convention – Bulgaria has implemented most of the provisions of the Palermo Convention. However, there are deficiencies in regards to implementation of Art. 6 (no clear definition of "property", not all of the designated categories of predicate offences are covered); Art. 12 (the seizure and confiscation could not be extended to the proceeds, instrumentalities used and intended for use in the commission of ML and TF, as well as legitimate property intermingled with the illegally obtained property) and Art. 18 (the shortcomings identified with respect to the provisional and the confiscation measures may have a negative impact on MLA requests. The practical application of dual criminality may limit Bulgaria's ability to provide assistance due to the shortcomings identified with respect to the ML offences).

Merida Convention – Bulgaria has implemented the Merida Convention mainly through the CC, CPC and LMML, as well as the LCCIAF.

Terrorist Financing Convention – Bulgaria has implemented the Terrorist Financing Convention and criminalized terrorist financing as required under Terrorist Financing Convention. Deficiencies identified in c.5.1 have an effect on the implementation of Terrorist Financing Convention by Bulgaria.

Weighting and Conclusion

There are deficiencies with implementation of Art. 5 of Vienna Convention, where the seizure and confiscation could not be extended to the instrumentalities used and intended for use in ML and TF and to the object of the crime in cases where the property is held by a third party, as well as legitimate property intermingled with the illegally obtained property. This deficiency is considerable taking into account widespread use of strawmen in Bulgaria. With regards to implementation of Art. 7, the shortcomings identified with respect to the provisional and confiscation measures may have a negative impact on MLA requests. Deficiencies in identified in R.3, 4 and 5 have effect on implementation by Bulgaria of Vienna and TF Conventions. **Recommendation 36 is rated LC**.

Recommendation 37 - Mutual legal assistance

In the 2013 MER, Bulgaria was rated LC with the previous R. 36. The assessment team considered that the shortcomings identified with respect to the provisional and confiscation measures may have a negative impact on MLA requests. Moreover, the application of dual criminality may limit Bulgaria's ability to provide assistance due to the shortcomings identified with respect of R1. Considering that R.36 was rated LC in the 4th round MER, Bulgaria has not informed of any developments in the course of the 4th round follow-up process.

Criterion 37.1 – Bulgaria has the legal basis to rapidly provide wide range of mutual legal assistance in relation to ML, associated predicate offices and TF. The legal framework of Bulgaria is comprised of a network of international treaties, conventions and EU Framework Decisions (directly applicable under national law), as well as local laws.

Art. 471 of the CPC provides that international legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance shall comprise the (1) service of process; (2) acts of investigation; (3) collection of evidence; (4) provision of information; (5) other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity.[118]

Criterion 37.2 – The central authority in Bulgaria for transmission and receipt of requests for international legal cooperation is the MoJ (see Art. 475 of the CPC). The procedure for submission and review of an MLA request is regulated in Articles 475 and 476 of the CPC. The PO has established clear rules and mechanisms for issuing and executing EAWs. There is no document that would govern timely execution of received MLA requests and sending requests for such assistance from Bulgarian investigative bodies to foreign authorities (non-EU) – both MoJ and PO ensure timely prioritisation and execution of MLAs on a case-by-case basis based on the professional qualifications of professionals handing MLAs.

In order to ensure timeliness, effectiveness and professionality in the execution of the requests on MLA, the PG issued an order[119] which established the International Department within the Supreme Cassation PO. This department deals only with international matters and cooperation. The correspondence or file received in the PO is registered in the registry office and is sent to the office in the respective unit in the system of the Prosecution, the information is entered in the Unified Information System (which serves as a case management system for the PO) of the Prosecution, distributed to the prosecutor who is supervising the case.

Criterion 37.3 – In Requests for MLA are not prohibited or made subject to unreasonable or unduly restrictive conditions. Art. 472 of the CPC sets out the ground for refusal of international legal assistance. In accordance with the relevant article international legal assistance may be refused if the implementation of the request could threaten the sovereignty, the national security, the public order and other interests, protected by law.

Criterion 37.4 – Bulgarian laws and regulations do not provide for grounds to refuse to execute a request for MLA in view of the fact that it involves fiscal matters or on the grounds of secrecy and confidentiality requirements of FIs or DNFBPs. There are no grounds for refusal of execution of MLA apart from those listed in Art. 472 of the CPC (see Criterion 37.3).

---

[118]Furthermore, the CPC also provides the following types of international assistance: (1) appearance of a witness and expert before a foreign court or foreign judicial bodies (see Article 473 of the CPC), (2) interrogation of individuals through a video or phone conference (see Article 474 of the CPC), (3) transfer of criminal proceedings (see Articles 478 and 479 of the CPC), (4) conducting parallel criminal proceedings (see Article 481 of the CPC), (5) application of special intelligence means in connection with international cooperation, (6) extradition and European arrest warrant (see Extradition and European Arrest Warrant Act), (7) joint investigation teams (see Article 476 of the CPC), (8) European Investigation Order (EIO) (see European Investigative Order Act) and other.

[119] Order No ЛС-3414 / 15.11.2013, (last amended by Order № РД-04-171 / 01.06.2020)

While there are no specific provisions of the CPC prescribing that under MLA information containing secrecy or confidentiality provisions may be provided to the requesting party, the bank and professional secrecy is regulated in Art. 62 of the Credit Institutions Law. The mentioned article provides that a public prosecutor can disclose necessary information should there be reason to believe that a criminal offence has been committed under Art. 31 of European Investigative Order Act (in such case a court of law may order disclosure of the information).

Criterion 37.5 – Art. 198 of the CPC provides that investigation materials may not be made public without authorisation by the prosecutor. There are other specific laws that also regulate the confidentiality matters for the execution of international requests or international cooperation (e.g., see Art. 23 of the European Investigative Order Act). According to the Internal rules for work with electronic documents of the MoJ, civil servants and officers in the relevant ministry are bound to keep secret the information which is available to them in the framework of their work.

Criterion 37.6 – In cases that do not involve coercive measures dual criminality is not a precondition for rendering MLA. The CPC does not list such a ground for refusing to provide mutual legal assistance. It is also evident from the declaration that Bulgaria has made to article 2 of the European Convention on Mutual Assistance in Criminal Matters (1959).

Criterion 37.7 – As there is no requirement for dual criminality for non-coercive measures the execution of MLA is not conditioned or limited by differences in the way countries denominate or categorise the offences. Dual criminality is only required in case of extradition and confiscation (see R.38 and R.39). Deficiencies identified in R.3 and R.5 apply to c.37.7.

Criterion 37.8 – Powers and investigative techniques that are required under Recommendation 31 or otherwise available to domestic competent authorities are performed by the competent national authorities when executing requests for MLA (see Section III of the CPC).

Weighting and Conclusion

For c.37.1 deficiencies identified in R.3 and R.5 apply. There is no document that would govern timely execution of received MLA requests and sending requests for such assistance from Bulgarian investigative bodies to foreign authorities (non-EU) (c.37.2). **R.37 is rated LC.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In the 2013 MER, Bulgaria was rated LC with the previous R. 38. The MER identified shortcomings with respect to enforcing foreign confiscation orders related to insider trading and market manipulation, as these offences are not properly criminalised in the national legislation. Another issue is the lack of a special asset forfeiture fund. Considering that R.38 was rated LC in the 4th round MER, Bulgaria has not informed of any developments in the course of the 4th round follow-up process.

Criterion 38.1 – The measures provided for in the Bulgarian laws and described under R. 4 appear to be equally available upon request of a foreign country as for local proceedings.

The legal framework in place gives the Bulgarian competent authorities a possibility to expeditiously act upon MLA requests to identify, freeze, seize, or confiscate property. For EU member states, this legal framework consists of the Law on recognition, execution and enactment of acts for securing property of 2006 (hereinafter the Law on Recognition of Acts) for the execution of foreign seizure/freezing orders (implementing Council Framework Decision 2003/577/JHA) and the Recognition, Execution and Transmission of Confiscation Orders and Decisions Imposing of Financial Sanction Act of 2010 (hereinafter the Recognition of Orders Act)

for the execution of foreign confiscation orders (implementing Council Framework Decision 2006/783/JHA). The said EU legal instruments have since been replaced by the EU Regulation 2018/1805 on the mutual recognition of freezing orders and confiscation orders, which is directly applicable in all EU Member States, including Bulgaria, for requests transmitted from 19.12.2020. All these instruments operate on a simplified certificate-based procedure with no dual criminality required for a broad range of serious criminal offences. For other crimes, both Bulgarian laws require dual criminality.

For non-EU countries, the general rules of MLA in Chapter 36 of the CPC apply. As for the receipt and execution of foreign seizure and freezing orders, Chapter 36 contains no specific procedural rules beyond the general provisions governing MLA in Art. 471 which is in stark contrast with the detailed procedures in the aforementioned EU (based) legal instruments. Specifically, there are no rules to provide for any expeditious action in this field. Dual criminality is not required by the CPC but, indirectly, by other international instruments in this field such as the 1959 European Convention on MLA (by means of a reservation made by Bulgaria).

Execution of foreign (non-EU) confiscation orders is provided by Art. 469 of the CPC which renders such orders executable pursuant to the general rules of recognition and enforcement of sentences issued by a foreign court, a formal court procedure with its respective deadlines (Art. 465). For the execution of a foreign confiscation order, dual criminality is required (Art. 463).

In accordance with Articles 53 and 253(6) of the CC, laundered property, proceeds, instrumentalities used in, and instrumentalities intended for use in a crime (or equivalent) can be confiscated. In cases of ML the object of crime or the property into which it has been transformed shall be forfeited to the benefit of the state, and where absent or alienated, its equivalent shall be awarded. In accordance with Art. 72 of the CPC, the Bulgarian court imposes security for the fine, confiscation and confiscation of property in favour of the state. This procedure is applied both in the pre-trial proceedings and for the laundered items, the benefits, the used funds and the funds used for ML/TF, as well as for securing the assets in order to return them to the legal owner. Deficiencies identified in criterion 1(b) and 1(c) of R.4 also apply here.

Criterion 38.2 – The confiscation measures under Art. 53 (1) CC apply irrespective of criminal liability and can thus be imposed also in lack of conviction (e.g., in case of the death of the perpetrator). On the other hand, the measures to secure the fine, confiscation, and forfeiture of objects to the benefit of the state set forth in the Code of Civil Procedure, which are to be applied in criminal procedures pursuant to Art. 72 CPC, require that the owner of the property, in respect of which the prosecutor has made a request for imposition of precautionary measures, be brought as an accused in the case, even if the measures themselves can be made *ex parte* and without prior notice – as a result of which they cannot be applied if the perpetrator is dead or unknown.

Criterion 38.3

a) Bulgaria has no specific measures in place that would regulate the possibility of arrangements for coordinating seizure and confiscation actions with other countries. In principle, and in light of the general provisions of the CPC, there are no restrictions for such arrangements.

b) As noted in criterion 4.4 mechanisms available for the active management of seized and confiscated assets are limited and do not go beyond storage and safekeeping measures. There are no mechanisms for managing and disposing of property that has been confiscated under CC.

Criterion 38.4 – Sharing of confiscated property with EU Member States is provided by Art. 28 of the Recognition of Orders Act (and Art. 30 of the new EU Regulation). As for non-EU member

states, the procedures or processes to share confiscated property can be done in accordance with international treaties that Bulgaria is part of. While the AT has no information on any specific treaty being in force in this field, they did not identify any obstacles preventing Bulgaria from signing such agreements.

Weighting and Conclusion

Deficiencies identified in c.4.1(b), c.4.1(c) and c.4.4 of R.4 are applicable in context of international cooperation. Provisional measures pursuant to Art. 72 CPC cannot be applied if the perpetrator is unknown or has dead. Bulgaria has no specific measures in place that would regulate the possibility of arrangements for coordinating seizure and confiscation actions with other countries, although there appear no restrictions for performing such actions. **R.38 is rated PC.**

Recommendation 39 – Extradition

In the 2013 MER, Bulgaria was rated C with the previous R.39.

Criterion 39.1 – Bulgaria's Extradition and European Arrest Warrant Act (hereinafter, EEAWA) specifies the conditions and procedure for effecting extradition to non-EU states, as well as the conditions and procedure for the issuance and execution of a European Arrest Warrant. The Republic of Bulgaria executes requests for extradition as well as surrender under European Arrest Warrants in a timely manner. Cases of immediate extradition are regulated in Art. 19 and Art. 45 of the EEAW, providing a procedure and timeline of immediate extradition cases.

(a) In accordance with Art. 5 of EEAWA, which stipulates the requirement for dual criminality, extradition shall only be granted where the act constitutes a criminal offence under Bulgarian law and under the law of the requesting State, which is punishable by deprivation of liberty or under a detention order for a maximum period of at least one year or by another more severe penalty. ML /TF offences fall into the scope of the said provisions, given the punishments for both of the offences prescribed by the CC. As Bulgaria requires dual criminality for extradition with non-EU countries, deficiencies in relation to criminalisation of TF offence would have impact on extradition (please see analysis of R.5). Additionally, extradition shall also be granted for the purpose of serving a prison sentence or a detention order by the person concerned, as made in the requesting State for a period of at least four months.

(b) The EEAWA provides a procedure for execution of extradition requests, as well as EAWs. The procedure is implemented through the specified Unified Information System, as well as according to the rules of the Instruction for extradition and EAW, of the PG of the Republic of Bulgaria.

(c) The conditions for the non-execution of requests as defined by the EEAWA do not appear unreasonable or unduly restrictive.

Criterion 39.2 – The extradition of Bulgarian citizens to a foreign (non-EU) country is inadmissible unless it is specifically provided by law or an international treaty. To date, Bulgaria has an agreement only with the United States, Norway, and Iceland. Surrender of Bulgarian nationals to other EU Member States is possible by means of a European Arrest Warrant. Based on an international treaty concluded by the EU and UK, Bulgaria can extradite its citizens to the UK.

(a) Pursuant to Art. 4 of the CC, no citizen of the Republic of Bulgaria can be transferred to another state or an international court of justice for the purposes of prosecution, unless this has been provided for in an international agreement, which Bulgaria is a party to. As per explanations of the country, Bulgarian citizens are not extradited to non-EU countries if there is no international

agreement. Also, in accordance with Art. 6 of the EEAWA the extradition of Bulgarian nationals shall not be granted, unless otherwise provided for in an international treaty to which the Republic of Bulgaria is a party. The said Art. also provides that the existence of Bulgarian nationality shall be determined at the moment of receipt of a request for extradition. Both provisions provide for the legal grounds for extradition of Bulgaria's nationals when it is stipulated for in an international treaty, to which Bulgaria is a state party and which has entered into force.

(b) Art. 21 of the EEAWA states that where the act is triable by a Bulgarian court, the records shall be made available to the respective prosecutor for the purposes of conducting a criminal prosecution, if there are grounds for this. The CPC also provides for the possibility to transfer a case where criminal proceeding has already been initiated (see Chapter thirty-six, Section IV). There are no explicit indications for cases to be submitted without undue delay. The AT did not find indications of any delays.

Criterion 39.3 – Pursuant to paragraph 3 of Art. 5, which sets out the requirements of dual criminality, an act shall constitute a criminal offence in both countries irrespective of the difference in the legal descriptions as long as the basic constituent elements of the offence coincide.

Criterion 39.4 – Several types of simplified extradition proceedings have been implemented in the laws of Bulgaria. E.g., pursuant to Art. 9 (2) of the Extradition and European Arrest Warrant Act a request for extradition can also be communicated through the diplomatic channel, Interpol or by other means of communication which may be arranged between the requesting state and Bulgaria. In accordance with Art. 18 (2) of the said Act, where a postponement may result in the expiry of the prescription period for prosecution in the requesting state or could seriously obstruct prosecution, the court may grant temporary extradition, provided the person is returned to Bulgaria immediately after performance of the steps in respect of which temporary extradition was granted. Additionally, Art. 19 of the EEAWA provides a simplified procedure in cases where consent is given to immediate extradition (also See Art. 45 and Art. 50 of the said Act).

Weighting and Conclusion

For c.39.1(a) deficiencies identified in R.5 apply. **R.39 is rated as LC.**

Recommendation 40 – Other forms of international cooperation

In the 2013 MER, Bulgaria was rated LC with the old R.38. The MER identified the following deficiencies: the BNB cannot exchange information with non-EU counterparts in the absence of an MoU; the FSC cannot exchange information with foreign counterparts in the absence of an MoU; no provisions enabling the BNB and FSC to perform direct enquiries on behalf of foreign counterparts. Considering that R.40 was rated LC in the 4th round MER, Bulgaria has not informed of any developments in the course of the 4th round follow-up process.

Criterion 40.1 – Section II of the LMML provides the possibility for the FID-SANS to exchange information internationally, including provisions pursuant to which FID-SANS is entitled to exchange any information at its disposal or to which it has direct or indirect access, including information on the natural and legal persons involved in the case, and information on the circumstances of the beneficial owners of legal persons and other legal entities. FID-SANS can exchange information with foreign FIUs both spontaneously and upon request and to exchange information both based on international treaties and based on reciprocity in cases of ML/TF or associated predicate offences.

Regarding the directorates within the SANS, the LSANS includes a general provision stating that the SANS shall engage in international cooperation relevant to its scope of activity. Further, the SANS can engage in international cooperation pursuant to international treaties to which the Republic of Bulgaria is a party.

International Operational Cooperation Directorate (IOCD) is the competent authority responsible for organisation and co-ordination of law enforcement information exchange internationally. The IOCD is the national contact point in the context of the INTERPOL, EUROPOL, ETIAS and the SIS. The IOCD is also responsible for bilateral information exchange via liaison officers' network under the concluded bilateral agreements for police cooperation. All national LEAs can also exchange information with their counterparts through the IOCD and vice versa. However, there is no explicit obligation under the Bulgarian law to provide assistance rapidly or in a timely manner, except for FIU-to-FIU cooperation under the LMML.

Criterion 40.2

(a) Bulgaria's competent authorities have a lawful basis for cooperation (see Criterion 40.1).

(b) and (c) Bulgarian legislative acts leave it to the competent authorities' discretion to determine the means and channels to be used for cooperation, including the most efficient ones. In particular, the FID-SANS uses the Egmont Secure Web and the FIU.Net system to exchange information with foreign counterparts. In regard to LEAs, IOCD is the competent authority responsible for organisation and co-ordination of law enforcement information exchange internationally, and IOCD exchanges information via INTERPOL, EUROPOL and via other information exchange channels.

(d) In the work of FID-SANS requests for information from foreign counterparts are subject to prioritization depending on the level of urgency and importance indicated by the requesting authority, case specifics, data required by the partner and the information currently available. Art. 90(3) of the LMML and Art. 14(2) of the LMFT, provide general provision for the time limits for the exchange of information. In regard to LEAs (SANS) there are no explicit legal provisions providing for timely exchange of information. The BNB's international co-operation timelines are explicitly stated in Bulgarian laws and regulation (*e.g.,* Art. 23 (4) of the LCI – regarding the period within which the BNB must communicate to the competent authority of the host Member State the information referred to in Art. 23(2) and (4) of the LCI).

(e) The measures for safeguarding the information for FID-SANS are described under the LMML Art. 93 and 39, LMFT and RILSANS. According to LMML, the information shall be exchanged over protected channels of electronic communication between the FIUs within the EU or the Egmont Group. Please refer to Recommendation 29 regarding the separate registers and practical information safeguards of the FID-SANS. Art. 2 (1) of the Classified Information Protection Act requires LEAs to safeguard foreign classified information which may be made available by another jurisdiction or an international organisation, insofar as an existing international treaty, to which the Republic of Bulgaria is a party, does not provide otherwise. Also, Chapter Seven of the act stipulates provisions for disclosure or exchange of classified information by the Republic of Bulgaria to, or with, another State or an international organisation. In regard to information of the BNB, these safeguards are covered with LCI and multilateral agreement between the ECB and AML/CFT competent authorities.

Criterion 40.3 – Pursuant to Art. 90(4) of LMML the FID-SANS has the possibility to negotiate non-binding agreements (*i.e.,* Memorandums of Understanding) with foreign FIUs which are members

of the Egmont Group. However, such an agreement is not a prerequisite of information exchange of the FID-SANS. Art. 90(1) of the LMML gives FID-SANS the opportunity to exchange information on the basis of international treaties and/or by reciprocity.

As regards to LEAs, bilateral or multilateral agreements are needed, Bulgaria has entered into such agreements with their relevant counterparts. There are no impediments for the authorities to enter into multilateral or bilateral agreements.

Criterion 40.4 – As regards to the FID-SANS, this requirement is addressed in Art. 93, para 4 of the LMML and Art. 14(2) of the LMFT. Feedback by the FID-SANS can and is provided both upon request and on FID-SANS own initiative. As a member of Egmont, the FID-SANS is bound by the Egmont Principles for Information Exchange, under which it provides feedback to foreign FIUs, upon request and also spontaneously. The feedback from the Bulgarian LEAs and/or prosecution is also included in the feedback to the foreign FIU.

As for LEAs, only general provisions regarding provision of feedback are in place. No reference has been made to the timeliness to be ensured by the authorities when providing feedback to their counterparts.

Criterion 40.5 – The conditions for the international exchange between FID-SANS and its foreign counterparts are listed in Articles 89-94 of the LMML and Art. 14(2) of the LMFT. FID-SANS is member of the Egmont Group and strictly follows the principles for exchange of information of this organization. The Bulgarian legislation does not set any restrictions for provision or exchange of information (please see specifically Art. 93(3) of the LMML and Art. 90(8) of the LMML). In regard to information exchange by the LEAs, there appear not to be any prohibitions or unreasonable restrictive conditions on the provision or exchange of information internationally. Art. 472 of the CPC stipulates the cases of refusal of international legal assistance, stating that international legal assistance may be refused if the implementation of the request could threaten the sovereignty, the national security, the public order and other interests, protected by law.

Criterion 40.6 – In relation to the FID-SANS Art. 93(2) of the LMML provides that it may use information only for the purpose for which the said information was requested or provided. Disclosure of any such information to another authority, institution or service or using any such information for purposes exceeding the initially approved purposes shall be subject to the prior consent of the counterpart FIU which has provided the information and in accordance with the conditions for exchange and use stated by the said FIU (see also Art. 14(2) of the LMFT).

For LEAs, the requirements of this criterion are covered by general confidentiality requirements of Art. 2(1) of the Classified Information Protection Act, which stipulates that the Act shall apply to any foreign classified information which may be made available by another State or an international organisation, insofar as an existing international treaty, to which the Republic of Bulgaria is a party, does not provide otherwise. Additionally, Chapter Seven of the said Act provides the requirements of disclosure or exchange of classified information by the Republic of Bulgaria to, or with, another jurisdiction or an international organisation.

Criterion 40.7 – FID-SANS applies the same safeguards for information received through international exchange as for domestically obtained information. In addition to domestic measures security requirements of the information exchange channels (FIU.NET and ESW) are applied. Moreover, foreign authorities need to provide their consent before obtained information can be disseminated. For LEAs, the requirements of this criterion are covered by general confidentiality requirements (see Criterion 40.6).

Criterion 40.8 – Art. 74 of the LMML and Art. 14(2) of the LMFT list the powers of FID-SANS to gather any type of information to which it has direct or indirect access when spontaneous dissemination or request from foreign FIU is received and for the purpose of analysis of the dissemination or answering the request. Also, the FID-SANS is authorised to conduct inquiries and obtain information on behalf of foreign counterpart FIUs (Art. 74, 89, 90 of LMML and Art. 14(2) of the LMFT).

For LEAs, competent authorities explained that directorates within SANS exercise inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts under European Investigation Order with the supervision of the competent Prosecutor Office. Additionally, competent authorities explained that the principle of availability and the principle of equivalent access set out in the Council Framework Decision 2006/960/JHA are transposed into the local legislation (Ministry of Interior a–t - Section II "Simplified Exchange of Information or Data with Competent Bodies of European Union (EU) Member States in View to Prevention, Detection and Investigation of Crimes" – art. 108 – 119).

Exchange of information between FIU

Criterion 40.9 – The FID-SANS has an adequate legal basis for providing co-operation on ML, associated predicate offences, as well as TF (see analysis in criterions 40.1 and 40.2).

Criterion 40.10 – As regards to the FID-SANS, this requirement is addressed in Art. 93, para 4 of the LMML and Art. 14(2) of the LMFT. Feedback by the FID-SANS can and is provided both upon request and on FID-SANS own initiative. As a member of Egmont, the FID-SANS is bound by the Egmont Principles for Information Exchange, under which it is required, upon request and whenever possible, to provide feedback to foreign counterparts. For more analysis see c.40.4.

Criterion 40.11 – The FID-SANS can exchange information with its counterpart FIUs abroad. This includes any information FID-SANS has access to or can obtain directly or indirectly (please refer to Art. 74 and 90(7) of the LMML and Art. 14(2) of the LMFT, as well as Criterion 29.3 under Recommendation 29).

Exchange of information between financial supervisors

Criterion 40.12 – LMML, Art. 128 permits each of the supervisory authorities to conclude written agreements with the competent supervisory authorities of the Member States for cooperation and exchange of information for the purposes of Directive (EU) 2015/849. However, this is legal provision is not applicable to third countries.

The FI supervisors have the following additional legal basis for cooperation:

The BNB has the legal basis for providing cooperation with the competent authorities of Member States participating in the SSM under Arts. 20(3) (regarding the banking system) and 20(4) regarding payment and e-money institutions) of the BNB Law; the ECB under Art. 121(e) of the BNB Law; the ECB, national central banks, competent authorities of Member States, the European Systemic Risk Board (ESRB), the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) under Art. 88 LCI (regarding credit institutions) and Art. 160a LPSPS (regarding other payment services). The BNB can enter into agreements with third countries under Arts. 66 LCI and 169a LPSPS and it is signatory to more than 20 multilateral and bilateral memoranda including MoUs with Banking Supervisors of South-Eastern Europe, the UK Financial Conduct Authority and the Bank of England.

The FSC can cooperate, exchange information and sign MoUs with foreign authorities exercising supervisory functions over financial market operations under Art. 13(1) FSCA. However, Art. 25 appears to limit information sharing to authorities in EU Member States. Further provisions are included within the MFIA and POSA (securities) and CISOUCIA (collective investment schemes), but these provisions do not extend to authorities other than those in Member States. The FSC is signatory to more than 70 multilateral and bilateral memoranda including an MoU concerning EEA competent authorities, the UK Financial Conduct Authority and the Bank of England, the IOSCO and the IAIS.

Regarding insurance supervision, the IC does not limit cooperation to Member States (Art. 279 which applies chapter 5 if the IC) and cooperation is not restricted by professional secrecy (Art. 273).

In relation to the pensions sector, there are no specific provisions regarding international cooperation in prudential legislation although the general provisions of the FSCA apply.

FID-SANS can cooperate and exchange information with authorities of the EU Member States on the basis of domestic law (Art. 3(8) LMML) and with other countries on the basis of international treaties and/or by reciprocity (Art. 90 LMML).

The following shortcomings exist therefore only FIDS-SANS is able to cooperate with foreign counterparts (regardless of their respective nature or status); (1) Art. 128 LMML permits supervisors to conclude agreements only with supervisory authorities of Member States; (2) the FSA is limited to sharing professional secrecy information with supervisory authorities of Member States.

Criterion 40.13 – The BNB can cooperate with the relevant competent supervisory authorities of EU Member States and disclose information that is essential for the exercise of its supervisory duties including information held by OEs that constitutes professional secrecy (Art. 160, Art. 159 LPSPS; Art. 65(2), Art. 95 LCI). The BNB can disclose professional secrecy information to the supervisory authorities of third countries on the basis of an agreement (Art. 88 LCI, Art. 160a LPSPS) and conditions of protection of the information, reciprocity, and use of information for supervision purposes (Art. 159a LPSPS; Art 66 LCI). The BNB MOUs referred to under c40.12 are sufficient to permit disclosure of information that constitutes professional secrecy.

The FSC to can provide information to the relevant competent authorities of EU Member States for the purpose of carrying out their duties (Art. 257 MFIA; Art. 100aa (1) POSA) and to share information with ESMA, ESRB, central banks, ECB and other relevant supervisory authorities regarding supervisory oversight of payment services (Art. 259, Art. 257 MFIA; Art. 25 FCSA). In addition, FSC can enter into agreements for cooperation and exchange of information with other supervisors of financial market (Art. 13(1) FCSA). However, the FSC MOUs referred to under c40.12 do not appear sufficient to permit disclosure of information that constitutes professional secrecy to the competent authorities of third countries.

FID-SANS may, in addition to exchanging information regarding ML/TF and predicate offences, disclose information to achieve objectives of Directive (EU) 2015/849 that is risk analysis ensuring effectiveness of system for preventing ML/TF. This does not restrict the disclosure of information that constitutes professional secrecy (Art. 90 LMML).

Criterion 40.14 – All supervisors are able to disclose information that constitutes professional secrecy to relevant supervisory authorities, thus covering items (a) to (c) of the criterion with the exception of the FSC MOUs referred to under c40.12, that do not appear sufficient to permit

disclosure of information that constitutes professional secrecy to the competent authorities of third countries.

Further, the certain prudential laws require cooperation regarding FIs that are part of a group. In particular, the BNB is required to cooperate with supervisors of EU Member States regarding group wide supervision (Art. 25(1), Art. 28(5), Art. 79a, Art. 87, Art. 92 LCI; for payment institutions and e-money providers Art.160 LPSPS, Arts. 32(12) and (13), Arts. 33(3) and (4) Art. 43 LPSPS).

For the FSC there are no specific provisions regarding cooperation amongst supervisors of groups within LPSPS or POSA however, the information sharing provisions described under c.40.13 are considered sufficient. The FSC cooperates with supervisory authorities in other EU Member States for the purpose of group supervision (including prudential) of the following entities: trading entities (Art. 253 MFIA), alternative investment funds (Art. 258 and Art. 252 CISOUCIA), vehicle for alternative insurance risk transfer (Art. 22(3), Art. 70, Art. 266, Art. 267, Art. 268, Art.269 IC), insurers and reinsurers (IC Art.231-285). The FSC MOUs referred to under c40.12 include detail on information sharing, joint supervision and regulatory colleges.

There are no specific provisions regarding cooperation amongst supervisors of groups within LMML however, the information sharing provisions in described under c.40.13 are considered sufficient.

Criterion 40.15 – The BNB and the relevant competent supervisor of a Member State shall cooperate regarding onsite inspections of credit institutions (Art. 87 LCI, establishing written agreements regarding arrangements including the delegation of responsibilities (Art. 94). Upon request from a supervisory institution of EU Member State, the BNB shall carry out verification of specific information and vice versa (Art. 100 LCI).

Regarding payment institutions, the BNB may carry out on-site inspections of entities licenced by another Member State to carry out payments' services and vice versa (Art. 32(14), Art. 33(5) LPSPS). Despite the general requirement to cooperate with the supervisory authorities of Member States, there is no explicit legal provision to permit the BNB to conduct inquiries of behalf of foreign counterparts or vice versa.

Arts. 43(5) to (7) LPSPS apply the group-supervision requirements to e-money institutions, therefore the shortcoming regarding conducting inquiries also applies. Despite the apparent lack of legal basis, the BNB MOUs referred to under c40.12 do allow the BNB to conduct inquiries on behalf of foreign counterparts and vice versa in order to facilitate effective group supervision.

There are no provisions in FSCA (generally) or POSA (securities) regarding the ability of the FSC to authorise or facilitate inquiries by foreign counterparts or vice versa for AML/CFT purposes. However, powers of FSC to request verifications and conduct investigations in other EU Member States and vice versa are contained in the following provisions: Arts. 256, Art. 256; Art. 272 MFIA; Art. 260; Art. 261 CISOUCIA; Art. 275 IC. Despite apparent shortcomings the FSC MOUs referred to under c40.12 are sufficient to allow the FSC to conduct enquiries on behalf of foreign counterparts or to authorise foreign counterparts to conduct investigations in order to facilitate effective group supervision.

There are no provisions in LMML regarding the ability of FID-SANS to authorise or facilitate inquiries by foreign counterparts or to conduct inquiries on behalf of foreign counterparts in order to facilitate effective group supervision.

Criterion 40.16 – The BNB and the FSC may reveal information representing a professional secret received by the authorities of a Member State or of a third country carrying out financial supervision only with their explicit consent and for the purposes for which this consent was given (Art. 64(3) LCI regarding credit institutions, Arts. 159(2) and 160 LPSPS (regarding other payment institutions and e-money institutions), Art.25(7) FSCA).

FID-SANS may reveal information to another party only for the purpose for which the said information was requested or provided except where there is prior consent from the FIU of the other country (Art. 93(2) LMML). However, this restriction appears to relate only to cooperation with FIUs and does not include supervisory cooperation.

Exchange of Information between Law enforcement authorities

Criterion 40.17 – Directorates within SANS exercise inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts under EIO with the supervision of the Prosecutor Office. The principle of availability and the principle of equivalent access set out in the Council Framework Decision 2006/960/JHA are transposed into the local legislation (Ministry of Interior act - Section II "Simplified Exchange of Information or Data with Competent Bodies of European Union (EU) Member States in View to Prevention, Detection and Investigation of Crimes" – Articles 108 – 119). The international exchange of information conducted by competent directorates within SANS involved in the prevention and counteraction to financial crime and counteraction of terrorism and its financing is based on internal instructions and agreements between SANS and MoI. Although, the AT was not provided copies/summaries of these internal instructions and agreements due to their confidential nature, during onsite this information was verified.

Criterion 40.18 – The relevant Bulgarian LEAs are authorised to conduct inquiries and obtain information on behalf of foreign counterparts (see also Criterion 40.8).

Criterion 40.19 – The Supreme Cassation Prosecution can establish together with other states joint investigation teams in which Bulgarian prosecutors and investigation authorities shall participate. An agreement with the competent authorities of the participant states shall be entered in respect of the activities, duration and composition of a joint investigation team. The joint investigation team shall comply with provisions of international agreements, the stipulations of the above agreement and Bulgarian legislation while being on the territory of the Republic of Bulgaria (please see Art. 476(3) of the CPC).

As per the competent directorates within SANS, competent authorities explained that JIT's with the involvement of Republic of Bulgaria are conducted under the supervision of Prosecutor Office of Bulgaria and SD of SANS shall execute concrete prosecutor's order, given in a JIT investigation.

Exchange of Information between non-counterparts

Criterion 40.20 – Regarding the FID-SANS, in accordance with Art. 90(1) of the LMML and Art. 14(2) of the LMFT, acting on its own initiative and on request, shall exchange information about a suspicion of ML/TF and about associated predicate offences with the relevant international authorities, authorities of the EU and authorities of other countries on the basis of international treaties and/ or by reciprocity. Therefore, exchange of information related to ML/TF and associated predicate offences can be conducted by FID-SANS with foreign competent authorities, regardless of if these are FIUs.

The IOCD is the competent authority responsible for organisation and co-ordination of law enforcement information exchange internationally. The IOCD is the national contact point in the

context of the INTERPOL, EUROPOL, ETIAS and the SIS. The IOCD is also responsible for bilateral information exchange via liaison officers' network under the concluded bilateral agreements for police cooperation. However, it is not clear if IOCD can exchange information with other competent authorities that are not their counterpart.

Weighting and Conclusion

Bulgaria has the following shortcomings in relation to R.40:there is no explicit obligation under the Bulgarian law to provide assistance rapidly or in a timely manner, except for FIU-to-FIU cooperation under the LMML (c.40.2); No specific provisions regarding cooperation amongst supervisors of groups within LPSPS, LMML or POSA (c.40.14); no explicit legal provision to permit the BNB to conduct inquiries on behalf of foreign counterparts or *vice versa* also in the MoUs (c.40.15.); there is no legal basis for supervisors to conclude agreements with non-EU Member States (c.40.12); the FSC can only share professional secrecy information with EU Member States and their MoUs do not permit disclosure of information that constitutes professional secrecy to the competent authorities of third countries (40.13); there are no provisions in FSCA (generally) or POSA (securities) regarding the ability of the FSC to authorise or facilitate inquiries by foreign counterparts or *vice versa* for AML/CFT purposes (c.40.15);restrictions on disclosure of information by FID-SANS does not extend to supervisory cooperation (c.40.16). There are also no provisions in LMML regarding the ability of FID-SANS to authorise or facilitate inquiries by foreign counterparts or to conduct inquiries on behalf of foreign counterparts in order to facilitate effective group supervision; regarding LEAs (SANS) there are no explicit legal provisions providing for timely exchange of information and only general provisions regarding provision of feedback are in place. **R.40 is rated LC.**

Summary of Technical Compliance – Deficiencies

ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	**LC**	• Bulgaria has deficiencies in relation to risk assessment, co-ordination and keeping the risk assessment up to date has not yet been demonstrated. • Not all activities that are covered by the FATF definitions for FI and VASP are subject to preventive and supervisory measures in Bulgaria and whilst DPMS are exempted from the AML/CFT requirements following the introduction of cash transaction threshold on the basis of risk, the exemption of other activities is not justified.
2. National cooperation and coordination	**PC**	• Bulgaria has deficiencies in relation to effective co-ordination mechanisms for developing and implementing national AML/CFT strategies and particularly ensuring that those strategies are adequately informed by risks. • There have not yet been any specific national policies developed based on risk understanding, apart from the actions contained in the 2019 NRA Action Plan which was only formally adopted during the onsite.
3. Money laundering offences	**LC**	• The criminal sanctions available for natural persons are dissuasive but the system of additional fines is not sufficiently proportionate. • There is no corporate criminal liability and the administrative liability of legal persons for criminal offences is limited.
4. Confiscation and provisional measures	**PC**	• Instrumentalities and intended instrumentalities of a criminal offence can only be confiscated from the perpetrator and not from third persons. • There is no clear provision for the confiscation of property "intended or allocated for use" in relation to TF. • Unless the respective object (property item) constitutes material evidence in the criminal proceedings (and thus can be subject of seizure pursuant to the CPC) the provisional measures cannot be applied before a formal accusation takes place and neither can they be applied to third parties (this also refers to the asset forfeiture proceedings by the CACIAF). • For the purposes of applying provisional measures in the criminal procedure, there is no explicit definition of property subject to these measures. • There is no mechanism available for the active management of seized and confiscated assets beyond storage and safekeeping measures, and for managing and disposing of property that has been confiscated under the CC.

Recommendations	Rating	Factor(s) underlying the rating
5. Terrorist financing offence	**PC**	• The TF offence has been amended to more comply with the FATF standards, but it still prescribes the purposive element for the TF offence, for all the offences, including the ones specified under the Conventions and Protocols listed in the Annex to the TF Convention. • It is still unclear whether the TF offence extends not only to funds but also to other assets. • Financing of travels to and from Bulgaria for the purpose of committing a terrorism-related act is not covered in its every aspect by the current legislation. • The range of punishment for TF has been lowered and the elimination of additional fines reduced the proportionality of the sanctions. • There is no corporate criminal liability and the administrative liability of legal persons for criminal offences is limited.
6. Targeted financial sanctions related to terrorism & TF	**PC**	• Designation criteria set out in the relevant UNSCRs, are not described under the mechanism of identifying targets for designation; there is no dedicated procedures in place, to address requirements of Criterion 6.1 c)-e). • The listing criteria as envisaged by the Art. 5(2) of LMFT do not fully correspond to the specific criteria, as set forth in UNSCR 1373. • There is no set timeline and no mechanism to consider that the request is supported by reasonable grounds, or a reasonable basis to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373. There is no formalized procedure under which Bulgaria could ask another country to give effect to freezing measures. • There is no procedure in place with regard to submitting de-listing requests, as well as to facilitate review by the 1988 Committee, and informing persons and entities of the availability of the UN office of Ombudsmen; there is no guidance for FIs, other persons or entities, on their obligations with respect to delisting or unfreezing actions.
7. Targeted financial sanctions related to proliferation	**PC**	• Main deficiencies identified are related to the absence of national procedures for the implementation of targeted financial sanctions in relation to proliferation.
8. Non-profit organisations	**PC**	• Bulgaria has not conducted a comprehensive analysis of NPO sector recently (last complex analysis was conducted in 2012). • Bulgaria has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors could abuse those NPOs. • No dedicated outreach was provided to the donor community.

Recommendations	Rating	Factor(s) underlying the rating
		• The monitoring or supervisory measures are applied to all NPOs regardless of TF risk.
9. Financial institution secrecy laws	**LC**	• Information exchange domestically is limited in scope; as well as international exchange of information by the supervisors (other than the FID-SANS) with the foreign counterparts. • Deficiencies exist in relation to the ability to request information in all circumstances and particularly in relation to TF and due to some financial and virtual assets related activities that fall outside the regulatory scope.
10. Customer due diligence	**PC**	• There are no explicit requirements: (i) to apply CDD where there is suspicion of TF; (ii) to carry out CDD other than identification and verification of identity where doubt arises regarding identity data; (iii) to verify the identity of a person acting on behalf of a customer and no legal provisions regarding cases where third parties are permitted to act without authorisation; (iv) to keep CDD "relevant" and to ensure that transactions are consistent with the OE's knowledge of the customer and its business; (v) understand the nature of the customer's business; (vi) to identify and take reasonable measure to verify the identity of a natural person who exercises control through other means than ownership in some circumstances; (vii) to adopt risk management procedures concerning conditions under which a customer may utilise the business relationship prior to verification; (viii) to take into account materiality and varying risks levels (except for higher risk customers and relationship); (ix) to conduct due diligence at appropriate times, taking whether and when CDD measures have been previously undertaken and the adequacy of data obtained; (x) to consider making a disclosure regarding TF; (xi) to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification. • Checks on source of funds apply only in relation to PEPs and high risk third countries. • The legislation allows for an operation or transaction to be carried out on behalf of and/or for the account of a third party without authorisation. • The legislation allows for an alternative method to identify and verify the legal persons and arrangements, i.e., not to request certified identity documents from the legal persons provided that legal personality information can be obtained from EU registers. • There are no requirements to verify the names of the relevant persons having senior management positions in the legal person or legal arrangement; • There are no explicit requirements to include the beneficiary of a life insurance policy as a relevant risk factor in determining

Recommendations	Rating	Factor(s) underlying the rating
		whether enhanced CDD measures are applicable for reasons other than being identified as a PEP. • There are no legal provisions to permit an OE not to complete CDD in cases where there is a ML/TF suspicion and reasonable belief that performing the CDD process will tip-off the customer.
11. Record keeping	**LC**	Deficiencies relating to the financial services exempted from the regulatory environment are relevant here.
12. Politically exposed persons	**PC**	• OEs are permitted (except where higher risks are identified) to solely rely on clients' declarations to determine the PEP status. In light of the context of Bulgaria, namely, prevalent corruption, this is considered a severe shortcoming and thus weighted most heavily. • There is no explicit requirement to conduct enhanced scrutiny on the whole business relationship with the policy holder before the pay-out when higher risks are identified. • Deficiencies relating to the financial services exempted from the regulatory environment are also relevant here.
13. Correspondent banking	**PC**	• Measures described under c.13.1-2 are not applied to credit institutions within the EU/EEA within Bulgarian law, except for higher risk Member States through the implementation of EBA Guidelines. • There is no requirement for the FIs to satisfy themselves that the respondent FI does not permit its accounts to be used by shell banks other than in ESA Guidelines.
14. Money or value transfer services	**PC**	• Paper-based vouchers and paper-based traveller's cheques which constitute "other stores of value" are exempted from the requirements. • No sanctions available for persons carrying out postal money orders without a licence (this excludes persons and entities whose licence has been previously revoked or suspended). • There is no requirement for agents of PMOs to be licensed or registered by the CRC or the PMO itself to maintain a current list of agents. • There are no explicit provisions to require inclusion of agents in AML/CFT programmes and monitoring.
15. New technologies	**PC**	• Implementation of the requirement to assess the risk of new technologies is not explicit but rather a prerequisite (dependent on whether or not new technologies-related risks are identified as high in the NRA or business wide risk assessment). • The following VASPS services are not covered: exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and administration of virtual assets or instruments enabling control over virtual assets participation

Recommendations	Rating	Factor(s) underlying the rating
		and provision of financial services related to an issuer's offer and/or sale of a virtual asset. • There are no legal provisions that would prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP. • There are no legal or regulatory measures in place to identify unregistered VASPs and apply sanctions for provision of unlicensed services. • Shortcomings identified under R.27, 34, 35, 37-40 apply to VASPs. • VASPs are not required to conduct CDD when occasional transaction is equal or exceeds €1 000 and no provisions exist requiring VASPs to comply with the elements of the R.16. • Shortcomings identified at R.6 and 7 equally apply to VASPs, namely at c.6.6(g), c.7.2(e), c.7.4(d) and 7.3.
16. Wire transfers	**LC**	• Paper-based vouchers and paper-based traveller's cheques which constitute "*other stores of value*" are not included in scope of MVTS. • There is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer, in cases where an MVTS provider controls both the sending and receiving end of the transfer.
17. Reliance on third parties	**C**	
18. Internal controls and foreign branches and subsidiaries	**PC**	• No established requirement to have policies and procedures on employee screening to ensure high standards when hiring. • Internal AML/CFT audit function is not mandatory. • Compliance with AML/CFT requirements via group-wide procedures is not mandatory, "*other means*" are permitted. • Disclosure of AML/CFT related data and information is permitted only for payment service providers, credit institutions and entities operating in insurance and securities market and does not cover other FIs. • There is no explicit requirement to share information regarding unusual activity and/or its analysis between group entities. • disclosure of information within a group is permitted only for certain types of FI. • There are no requirements to have group wide programmes on adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Recommendations	Rating	Factor(s) underlying the rating
		• Requirement to ensure that foreign branches and subsidiaries apply AML/CFT measures consistent with the home country requirements do not extend to EU countries. • The legislation does not explicitly cover a scenario where AML/CFT requirements of the host country are less strict than those of the home country. • Deficiencies relating to the services exempted from the regulatory environment also apply here.
19. Higher-risk countries	**LC**	• No explicit reference in the legislation to high risk third countries identified by the FATF, including the "*counter measures list*". • No explicit requirement for enhanced CDD to be proportionate to the risks. • Published high-risk country lists are not entirely aligned with the FATF lists. • Deficiencies relating to the services exempted from the regulatory environment also apply here.
20. Reporting of suspicious transaction	**LC**	• There is no explicit requirement to report in cases where there are *reasonable grounds* to suspect ML/TF. • Deficiencies relating to the services exempted from the regulatory environment also apply here.
21. Tipping-off and confidentiality	**LC**	• There are no explicit legal requirements relating to safeguards on the confidentiality of information exchanged, specifically regarding safeguards of tipping off prevention. • Limitations apply concerning information sharing between group entities relating to unusual activities.
22. DNFBPs: Customer due diligence	**PC**	• Deficiencies identified in the following Recommendations are equally applicable under R.22: R.10 (PC), R.11(LC), R.12 (PC), R.15 (PC) and R.17 (C) which are relevant to DNFBPs.
23. DNFBPs: Other measures	**LC**	• Deficiencies identified in the following Recommendations are equally applicable under R.23: 18 (PC), 19(LC), 20(LC), 21(LC) which are relevant to DNFBPs.
24. Transparency and beneficial ownership of legal persons	**PC**	• Bulgaria has conducted high level risk assessment of legal persons, however, ML/TF risks associated with all types of legal persons have not been comprehensively assessed. • There are no specific provisions in Bulgaria to ensure that basic information required at c.24.4 is always maintained by the companies within the country at a location notified to the companies' registry. • There are not sufficient mechanisms in Bulgaria to ensure accuracy of the basic information. • Minor shortcomings concerning BO definition identified at c.10.5 have an impact on criterion c.24.6.

Recommendations	Rating	Factor(s) underlying the rating
		• There are no sufficient regulatory measures to ensure (verify) accuracy of the BO information. • Authorities and legal persons themselves are not required to maintain the information and records for at least five years after the date on which the company is dissolved or ceases to exist. • Bulgaria has taken steps to legally require bearer shares conversion into the registered shares by mid-2019, however, the exercise has not been completed to date. • The sanctions for persons that fail to comply with the requirements are not proportionate or dissuasive in all circumstances. • There are no mechanisms in the country to prevent nominee misuse.
25. Transparency and beneficial ownership of legal arrangements	**PC**	• Professional trustees of foreign law trusts are not required to disclose their status to FIs/DNFBPs when forming a business relationship or carrying out an occasional transaction. • No explicit power is provided in the legislation for to allow competent authorities to use their investigative powers to obtain beneficial ownership information on behalf of foreign counterparts. • Sanctions applicable to trustees for failure to meet their obligations in relation to CDD, record keeping and providing information to the registry are not considered to be fully dissuasive and proportionate. • There are no explicit sanctions for professional trustees for failing to grant timely access to information to the competent authorities.
26. Regulation and supervision of financial institutions	**PC**	• Some financial services fall outside the scope of licensing and supervision: paper-based vouchers and paper-based traveller's cheques (except where provided by a bank) and safekeeping. • Entry controls of all FIs do not explicitly prohibit licensing /registration in case of association with criminals; number of various other shortcomings established in licensing requirements relate to the absence of explicit requirements regarding non-criminality, as well as rehabilitation, etc. • Due to multiple shortcomings under c.26.5 these are collectively considered moderate: there is no explicit requirement to determine frequency and intensity of supervision on the basis of characteristics of the FIs and financial groups, incl. diversity, number, etc. Moreover, it is not explicit that the above listed criteria should be cumulatively used to determine the frequency and intensity of the on-site and off-site supervision; In addition, it is not explicit that data discussed at c.26.5(a) and c.26.5(b) is used by the supervisory

Recommendations	Rating	Factor(s) underlying the rating
		authorities with a view to determine the frequency and intensity of the on-site and off-site supervision. • Regulation and supervision of FIs (that fall outside the scope of core principle institutions and PIs/EMIs) demonstrates notable shortcomings and does not appear to have regard to the ML/TF risks. Moreover, regulation and supervision of currency exchange providers by the NaRA and postal money operators by the CRC is not risk based and systems for supervisory monitoring are underdeveloped. • Supervisors are not explicitly required to assess the ML/TF risk profile of an individual financial institution or group, including the risk of non-compliance.
27. Powers of supervisors	**PC**	• The legal basis for supervision, incl. on-site inspections by NaRA (regarding currency exchange) and CRC (regarding postal operators) is not explicitly established. • LMFT does not include provisions to compel production of information regarding compliance with LMFT by the supervisory authorities other than FID-SANS and BNB. • Per R.35: proportionate and dissuasive sanctions for non-compliance with LMML and LMFT are not available in all cases.
28. Regulation and supervision of DNFBPs	**PC**	• Beneficial ownership threshold regarding entry controls for gambling operators is higher than permitted by the Standard. • No market entry controls with a view to prevent criminals from entering the market exist for real estate agents and TCSPs, and very limited controls for accountants/auditors. • Entry controls do not cover criminal association for all types of DNFBPs. • No market entry conditions legally established regarding the ownership, control or management in DNFBPs other than casinos/gambling entities. • Joint Instruction between FID-SANS and NaRA (regarding gambling) covers only LMML compliance and not LMFT compliance and supervision is not risk-based. • Regulatory processes regarding risk-based supervision of DNFBPs by FID-SANS are under development thus compliance with c.28.5 cannot be demonstrated. • No supervisors have legal powers to supervise TFS related to PF by DNFBPs.
29. Financial intelligence units	**LC**	• There is a separate parallel reporting system for everyone who has knowledge of TF to Chairperson of SANS and MoI (Art. 9(1) of the LMFT). • Neither the LMML nor LMFT cover circumstances where there are reasonable grounds to suspect, which potentially might limit the information reported to FID-SANS by the OEs.

Recommendations	Rating	Factor(s) underlying the rating
		• There are also some minor issues that can affect the autonomy of FID-SANS and concerns regarding the budget allocation to FID-SANS.
30. Responsibilities of law enforcement and investigative authorities	**LC**	• The mechanism available for identifying and tracing property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime by the CACIAF cannot be considered expeditious as required by c.30.3
31. Powers of law enforcement and investigative authorities	**C**	
32. Cash couriers	**PC**	• The criminal sanctioning regime is incomplete as it only exists for large-scale cases of non-compliance at the external EU borders. • Temporarily retainment of cash in the sense of c.32.8 is only formally provided at the EU external borders, but domestic legislation for the practical application of this mechanism is still not in place, while there is no such mechanism at all for the EU internal borders, as a result of which there are currently no legal powers for the detention of cash suspected to be linked to ML/TF.
33. Statistics	**PC**	• Bulgaria does not maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system.
34. Guidance and feedback	**PC**	• FID-SANS published guidance is generic and not tailored to specific FI/DNFBP types; in general, very limited consolidated feedback is being provided by FID-SANS to the OEs to assist them in detecting and reporting suspicious transactions. • Guidance on specific red flags has been provided only to banks, other sectors have not been covered. • There is currently no guidance other than links to European Guidance published by the BNB, the FSC, the NaRA or the CRC. • No outreach has been carried out by the NaRA or the CRC either independently or jointly with FID-SANS.
35. Sanctions	**PC**	• Criminal Code does not provide for more dissuasive penalties for more serious crimes. • Criminal Code applies only to the LMML violations and not to the LMFT violations. • The FSC is not able to restrict (as opposed to revoke) a licence. • The FSC is only able to revoke licence regarding the LMML violations and not for the LMFT violations, however, no powers to revoke a license of an AIM. • The FSC has no legal basis for issuing written warnings or orders to address violations.

Recommendations	Rating	Factor(s) underlying the rating
		• The NaRA (regarding gambling) has no legal basis to sanction other than imposition of administrative financial penalties. • Monetary penalties applicable to directors and senior management are not fully dissuasive. • Sanctions for non-compliance with the TFS related to TF requirements do not appear fully dissuasive, especially with respect to maximum amount of fine applicable to OEs. • No sanctions are available for non-compliance with TFS related to PF.
36. International instruments	**LC**	• There are deficiencies with implementation of Art. 5 of Vienna Convention, where the seizure and confiscation could not be extended to the instrumentalities used and intended for use in the commission of ML and TF and to the object of the crime in cases where the property is held by a third party, as well as legitimate property intermingled with the illegally obtained property. • With regards to implementation of Art. 7, the shortcomings identified with respect to the provisional and confiscation measures may have a negative impact on MLA requests. • Deficiencies in identified in Recs. 3, 4 and 5 have effect on implementation by Bulgaria of Vienna and TF Conventions
37. Mutual legal assistance	**LC**	• For c.37.1 deficiencies identified in R.3 and R.5 apply. • There is no document that would govern timely execution of received MLA requests and sending requests for such assistance from Bulgarian investigative bodies to foreign authorities (non-EU).
38. Mutual legal assistance: freezing and confiscation	**PC**	• Deficiencies identified in c.4.1(b), c.4.1(c) and c.4.4 of R.4 are applicable in context of international cooperation. • Provisional measures pursuant to Art. 72 CPC cannot be applied if the perpetrator is unknown or has dead. • Bulgaria has no specific measures in place that would regulate the possibility of arrangements for coordinating seizure and confiscation actions with other countries, although there appear no restrictions for performing such actions.
39. Extradition	**LC**	• For c.39.1(a) deficiencies identified in R.5 apply.
40. Other forms of international cooperation	**LC**	• There is no explicit obligation under the Bulgarian law to provide assistance rapidly or in a timely manner, except for FIU-to-FIU cooperation under the LMML. • There is no specific provisions regarding cooperation amongst supervisors of groups within LPSPS, LMML or POSA. • There is no no explicit legal provision to permit the BNB to conduct inquiries on behalf of foreign counterparts or *vice versa* also in the MoUs.

Recommendations	Rating	Factor(s) underlying the rating
		• There is no legal basis for supervisors to conclude agreements with non-EU Member States. • The FSC can only share professional secrecy information with EU Member States and their MoUs do not permit disclosure of information that constitutes professional secrecy to the competent authorities of third countries. • There are no provisions in FSCA (generally) or POSA (securities) regarding the ability of the FSC to authorise or facilitate inquiries by foreign counterparts or *vice versa* for AML/CFT purposes. • Restrictions on disclosure of information by FID-SANS does not extend to supervisory cooperation. • There are also no provisions in LMML regarding the ability of FID-SANS to authorise or facilitate inquiries by foreign counterparts or to conduct inquiries on behalf of foreign counterparts in order to facilitate effective group supervision regarding LEAs (SANS) there are no explicit legal provisions providing for timely exchange of information and only general provisions regarding provision of feedback are in place.

GLOSSARY OF ACRONYMS[120]

AML	Anti-money laundering
AML/CFT	Anti-Money Laundering/Countering Financing of Terrorism
Art.	Article
BCP	Border Crossing Point
BGN	Bulgarian Leva
BNI	Bearer-negotiable instruments
BNB	Bulgarian National Bank
BNB-SSAD	Bulgarian National Bank Specific Supervisory Directorate of the Banking Supervision Department
BNB-MFM	Bulgarian National Bank Specific Oversight of Payment Services Division of the Methodology and Financial Markets Directorate
BO	Beneficial Owner
BSE	Bulgarian Stock Exchange
C	Compliant
CC	Criminal Code
CD	Central Depository (Securities Registrar)
CDD	Customer Due Diligence
CDCOC	Chief Directorate Combating Organised Crime
CDNP	Chief Directorate "National Police"
CEPACA	Commission for establishing property, acquired from criminal activity
CEP	Compliance Enhancing Procedures
CETS	Council of Europe Treaty Series
CPDP	Commission for Personal Data Protection
CRS	Common Reporting Standard
CFSP	Common Foreign and Security Policy
CFT	Combating the financing of terrorism
CIS	Collective investment schemes
CL	Currency Law
CoE	Council of Europe
CPC	Criminal Procedure Code (Code of Criminal Procedure)
CTCC	Counter-terrorism Coordination Centre
CTR	Cash transaction report
DNFBP	Designated Non-Financial Businesses and Professions
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
EAW	European Arrest Warrant
EEA	European Economic Area
EEAWA	European Arrest Warrant Act
EC	European Commission

120 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

EDD	Enhanced Customer Due Diligence
EJN	European Judicial Network
EMI	Electronic Money Institution
EBA	European Banking Authority
ESA	European Supervision Authority
ESW	Egmont Secure Web
ETS	European Treaty Series
EU	European Union
EUR	Euro
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FSC	Financial Supervision Commission
FI	Financial Institution
FID-SANS	Financial Intelligence Directorate of State Agency for National Security
FIU	Financial Intelligence Unit
FSC	Financial Supervision Commission
GDP	Gross domestic product
GRECO	Group of States against Corruption
IO	Immediate Outcome
IODC	International Operational Cooperation Directorate
IRRC	Investment-related residence and citizenship
JSC	Joint Stock Companies
LEA	Law Enforcement Agency
LCI	Law on Credit Institutions
LCPA	Limitation of Cash Payments Act
LCCIAF	Law for Combating Corruption and Illegal Assets Forfeiture
LLC	Limited Liability Company
LMFT	Law on the Measures Against the Financing of Terrorism
LMML	Law on the Measures Against Money Laundering
LPSPS	Law on Payment Services and Payment Systems
LSANS	Law on State Agency for National Security
MAAC	Multilateral Convention
MER	Mutual Evaluation Report
MFA	Ministry of Foreign and Political affairs
ML	Money Laundering
MLA	Mutual Legal Assistance
MoI	Ministry of Interior
MoJ	Ministry of Justice
MoU	Memorandum of Understanding
MVTS	Money or Value Transfer Services
NPO	Non-profit organisation
NRA	National Risk Assessment
NaRA	National Revenue Agency
OCG	Organised criminal group
OE	Obliged entity

OEA	Office for Economic Activities
OECD	Organisation for Economic Co-operation and Development
PEP	Politically exposed person
PF	Proliferation financing
PI	Payment Institution
PMO	Postal money order (operators)
PO	Prosecutors Office
PoC	Point of contact
PSP	Payment service provider
RBA	Risk-based approach
RBS	Risk-based supervision
REAs	Real estate agents
RILMML	Rules on Implementation of the Law on the Measures Against Money Laundering
RILSANS	Rules on Implementation of the Law on State Agency for National Security
SANS	State Agency for National Security
SCDD	Simplified Customer Due Diligence
SOF	Source of funds
SOW	Source of wealth
SPA	Joint-stock company
SRB	Self-regulatory body
SRL	Limited liability company
STR	Suspicious transaction report
TC	Technical compliance
TCSP	Trust and Company Service Provider
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolution
VAs	Virtual assets
VASP	Virtual Assets Services Provider
4th AMLD	Directive (EU) 2015/849 of the European Parliament and of the Council
5th AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council

www.coe.int/MONEYVAL

May 2022

Anti-money laundering and counter-terrorism financing measures

Bulgaria

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Bulgaria as at the date of the on-site visit (6 to 17 September 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Bulgaria AML/CFT system and provides recommendations on how the system could be strengthened.