

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(2024)1

Anti-money laundering and counter-terrorist financing measures

Bulgaria

1st Enhanced Follow-up Report & Technical Compliance Re-Rating

May 2024

Follow-up report



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 1st Enhanced Follow-up Report and Technical Compliance Re-Rating on Bulgaria was adopted by the MONEYVAL Committee through written procedure (21 May 2024).

All rights reserved. Reproduction of the texts in this publication is authorised provided the full title and the source, namely the Council of Europe, are cited. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc.) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg or moneyval@coe.int)

Bulgaria: First Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER) of Bulgaria was adopted in May 2022. Given the results of the MER, Bulgaria was placed in enhanced follow-up.¹ The report analyses the progress of Bulgaria in addressing the technical compliance (TC) deficiencies identified in its MER. Re-ratings are given where sufficient progress has been made. Overall, the expectation is that countries will have addressed most if not all TC deficiencies by the end of the third year from the adoption of their MER.

2. The assessment of the request of Bulgaria for technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur teams (together with the MONEYVAL Secretariat):

- Armenia
- Azerbaijan
- Croatia
- Cyprus

3. Section II of this report summarises the progress of Bulgaria made in improving technical compliance. Section III sets out the conclusion and a table showing which Recommendations have been re-rated.

II. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

4. This section summarises the progress made by Bulgaria to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER for which the authorities have requested a re-rating (Recommendation (R.)2, R.12, R.13, R.14, R.15, R.18, R.22, R.25, R.26, R.27, R.32, and R.33).

5. For the rest of the Recommendations rated as partially compliant (PC) (R.4, R.5, R.6, R.7, R.8, R.10, R.24, R.28, R.34, R.35, and R.38) the authorities did not request a re-rating.

6. This report takes into consideration only relevant laws, regulations or other anti-money laundering and combating financing of terrorism (AML/CFT) measures that are in force and effect at the time that Bulgaria submitted its country reporting template – at least six months before the follow-up report (FUR) is due to be considered by MONEYVAL.²

II.1 Progress to address technical compliance deficiencies identified in the MER

7. Bulgaria has made progress to address the technical compliance deficiencies identified in the MER. As a result of this progress, Bulgaria has been re-rated on R.2, R.12, R.14, R.18, R.22, R.25, R.26, R.27, R.32 and R.33. The country asked for re-ratings for R.13 and R.15 which are also analysed but no re-rating has been provided.

8. Annex A provides the description of the country's compliance with each Recommendation that is reassessed, set out by criterion, with all criteria covered. Annex B provides the consolidated list of remaining deficiencies of the re-assessed Recommendations.

1. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.

2. This rule may be relaxed in the exceptional case where legislation is not yet in force at the six-month deadline, but the text will not change and will be in force by the time that written comments are due. In other words, the legislation has been enacted, but it is awaiting the expiry of an implementation or transitional period before it is enforceable. In all other cases the procedural deadlines should be strictly followed to ensure that experts have sufficient time to do their analysis.

III. CONCLUSION

9. Overall, in light of the progress made by Bulgaria since its MER was adopted, its technical compliance with the Financial Action Task Force (FATF) Recommendations has been re-rated as follows:

Table 1. Technical compliance with re-ratings, May 2024

R.1 LC	LC (FUR1 2024) PC	R.3 LC	R.4 PC	R.5 PC
R.6 PC	R.7 PC	R.8 PC	R.9 LC	R.10 PC
R.11 LC	LC (FUR1 2024) PC	R.13 PC (FUR1 2024) PC	C (FUR1 2024) PC	R.15 PC (FUR1 2024) PC
R.16 LC	R.17 C	R.18 LC (FUR1 2024) PC	R.19 LC	R.20 LC
R.21 LC	R.22 LC (FUR1 2024) PC	R.23 LC	R.24 PC	LC (FUR1 2024) PC
R.26 LC (FUR1 2024) PC	R.27 LC (FUR1 2024) PC	R.28 PC	R.29 LC	R.30 LC
R.31 C	R.32 C (FUR1 2024) PC	R.33 C (FUR1 2024) PC	R.34 PC	R.35 PC
R.36 LC	R.37 LC	R.38 PC	R.39 LC	R.40 LC

Note: There are four possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC), and non-compliant (NC).

10. Bulgaria will remain in enhanced follow-up and will continue to report back to MONEYVAL on progress to strengthen its implementation of AML/CFT measures. Bulgaria is expected to report back within one year's time.

Annex A: Reassessed Recommendations

Recommendation 2 - National Co-operation and Co-ordination

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.2. Following deficiencies were identified: (i) 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; (ii) there had 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 onsite.

2. **Criterion 2.1** – Art. 96 (1) – (4) of the Law on the Measures Against Money Laundering (LMML) establishes a standing interdepartmental working group – NRAM WG (see also c.1.2), which amongst its other duties: (i) conducts and updates national and sectorial risk assessments; and (ii) provides proposals on measures to be taken to mitigate the identified risks, including measures related to the allocation of resources and on the action plan for prevention and/or mitigation of those risks, to the Council of Ministers.

3. The Strategy for Countering Money Laundering and Terrorism Financing in the Republic of Bulgaria 2023-2027 (the Strategy) establishes the priorities and defines the key actions through which to fulfil those priorities, taking into consideration the findings of the national, as well as sectorial risk assessments. The Strategy was approved by the Council for Coordination and Cooperation - chaired by the Prime Minister and tasked with the high-level co-ordination and monitoring of activities in the AML/CFT field (Council of Ministers Decree No. 101 of 14 July 2023) - and subsequently adopted by the Council of Ministers (Council of Ministers Decision No. 586 of 31 August 2023). The Council for Coordination and Cooperation is also tasked with the control and overview of the implementation of various action plans in the field of AML/CFT. The Action Plan for the implementation of the Strategy, which is aimed at addressing the risks and vulnerabilities identified in the National Risk Assessment (NRA) was approved on 23 November 2023 by the Council for Coordination and Cooperation and subsequently adopted by the Council of Ministers (Council of Ministers Decision No. 66 of 31 January 2024). The Action Plan establishes implementing measures, as well as the timeframe to address those measures.

4. **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 co-ordination mechanism in the area of AML/CFT policy.

5. **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.

6. Co-ordination 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 co-operation.

7. 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 Rules on Implementation of the Law on the Measures Against Money Laundering (RILMML) regarding reports to the Council of Ministers.

8. **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.

9. With an act of the Council of Ministers No 50/01.03.2012 the State Agency for National Security (SANS) is appointed to carry out the counterproliferation co-ordination 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 organisation. 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 co-operation 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.

10. **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.

11. Representatives of the Commission for Personal Data Protection participated in meetings of the ad-hoc working group (mentioned in c.2.2) in relation to the transposition of Directive (EU) 2015/849 of the European Parliament and of the Council (4th AMLD) and Directive (EU) 2018/843 of the European Parliament and of the Council (5th AMLD) where the elements of personal data protection were considered.

12. The relevant provisions of LMML and Law on the Measures Against the Financing of Terrorism (LMFT) that take into consideration the requirements of the General Data Protection Regulation are Art. 83 and paragraph 4 of the supplementary provisions of LMML and paragraph 1c of the supplementary provisions of the LMFT.

Weighting and Conclusion

13. While Bulgaria has measures in place addressing the requirements of R.2, there is a following shortcoming relating to c.2.4: despite the fact that the SANS is appointed to carry out the counter proliferation co-ordination between the competent authorities, there are no specific co-operation and co-ordination mechanisms to combat PF on the operational level. Despite this moderately weighted shortcoming, the overall level of compliance with R.2 is largely achieved. For these reasons, **R.2 is rated largely compliant.**

Recommendation 12 – Politically exposed persons

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.12. The assessment identified some technical deficiencies related to reliance on clients' declarations to determine the PEP status; and the lack of requirements for enhanced scrutiny on the whole business relationship with the policy holder before the pay-out when higher risks are identified.

2. **Criterion 12.1** – Art. 36(1) of the LMML requires obliged entities (OEs) to apply enhanced Customer Due Diligence (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 Beneficial Owner (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 Beneficial Owner (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 Enhanced Due Diligence measures, obtaining a written declaration from the customer on PEP status and/or relying on information obtained by using internal or external databases. At the same time, Art. 42(3) of the LMML does not allow a written declaration from the customer on PEP status to be the only source of information when determining whether a customer or the BO of a customer is a PEP. Art. 25 of the RILMML 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. Under Supplementary Provisions (paragraph 1 – items 28 and 29), the LMML defines the terms “source of funds” and “source of wealth”. In addition, a guidance is provided by the European Supervision Authority which is applicable to entities supervised by the Bulgarian National Bank (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.

3. **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.

4. **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.

5. **Criterion 12.4** – Art. 43 of the LMML requires insurers, insurance intermediaries, credit and financial institutions 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.

6. 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) and (4) of the LMML requires senior management to be notified of a person being identified as a PEP prior to pay-out and requires the OE to consider making a disclosure to the Financial Intelligence Directorate of State Agency for National Security (FID-SANS) and to carry out an enhanced scrutiny and analysis of the business relationship before proceeding with the payments. These measures refer to all policies where BOs or beneficiaries are identified as PEPs and not only to ones where higher risks are identified, since the LMML doesn't prescribe higher risk as a precondition for their application. However, the enhanced scrutiny measures do not explicitly apply to whole business relationship.

Weighting and Conclusion

7. There is no explicit requirement to conduct enhanced scrutiny on the “whole” business relationship with the policy holder before the pay-out (c.12.4). **R.12 is re-rated largely compliant.**

Recommendation 13 – Correspondent banking

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)

1. In the 2022 MER, Bulgaria was rated PC on R.13. The assessment identified some technical deficiencies related to application of measures to credit institutions within the EU/EEA, except for higher risk Member States, and measures for the Financial Institutions (FIs) to satisfy themselves that the respondent FI does not permit its accounts to be used by shell banks.

2. 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.

3. **Criterion 13.1** – Art. 44 of the LMML requires OEs (including FIs), to apply the following measures before establishing correspondent relationships:

- (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 Money laundering/terrorist financing (ML/TF) investigation or supervisory measures (regulatory actions). Only the first part of this measure (gathering sufficient information about a respondent institution to understand fully the nature of the respondent’s business) applies to respondent institutions from third countries as well as to respondent institutions from EU/European Economic Area (EEA) Member States (Art. 44(1)(3) of the LMML) and the rest (determine from publicly available information the reputation of the institution and the quality of the supervision, including where it has been subject to ML/TF investigation or supervisory measure (regulatory actions) applies to respondent institutions from: (i) third countries (Art. 44(2)(1) of the LMML); and (ii) EU/EEA Member States when a higher risk is identified (Art. 44(4) of the LMML).
- (b) assess the respondent institution’s AML/CFT controls. This measure applies to respondent institutions from: (i) third countries (Art. 44(2)(2) of the LMML); and (ii) EU/EEA Member States, when a higher risk is identified (Art. 44(4) of the LMML).
- (c) obtain approval from senior management before establishing new correspondent relationships (Art. 44(1)(2) of the LMML); and
- (d) define and document the respective AML/CFT responsibilities of each institution. This measure applies to respondent institutions from: (i) third countries (Art. 44(2)(2) of the LMML); and (ii) EU/EEA Member States, when a higher risk is identified (Art. 44(4) of the LMML).

4. **Criterion 13.2** – Art. 44 (3) of the LMML (Amended, SG No. 84/2023) 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.

5. 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.

6. **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(3) prohibits the OEs from establishing and maintaining correspondent relationship with an institution outside Bulgaria that allows its accounts to be used by shell banks.

7. Art. 45(2) of the LMML states that when establishing correspondent relationships with institutions from other countries, OEs shall collect sufficient information about the respondent institution to ensure that the respondent institution does not allow its accounts to be used by shell banks.

Weighting and Conclusion

8. Bulgaria meets some of the requirements for correspondent banking, but requirements to: (i) determine from publicly available information the reputation of the institution and the quality of the supervision, including where it has been subject to a ML/TF investigation or supervisory measure (regulatory actions); (ii) assess the respondent institution's AML/CFT controls; and (iii) define and document the respective AML/CFT responsibilities of each institution apply to respondent institutions from EU/EEA Member States only when a higher risk is identified. Bearing in mind the materiality of correspondent relationships with EU/EEA Member States, **R.13 remains rated partially compliant.**

Recommendation 14 – Money or value transfer services

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ C (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.14. The assessment identified some technical deficiencies related to exemption of some types of “other stores of values” from the requirements; sanctions for persons carrying out postal money orders without a licence; requirements for registration/licensing/maintaining the list of agents and inclusion of those into the AML/CFT programmes and monitoring.

2. **Criterion 14.1** – The following types of payment services listed at Art. 4 of the Law on Payment Services and Payment Systems (LPSPS) fall under the scope of Money or value transfer services (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.

3. 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 Communications Regulation Commission (CRC) under Art. 39 of the Postal Services Act. The Postal Services Act (amended by SG 84/2023) clarifies that only legal persons or sole traders who perform one or more postal services and are registered under the legislation of the Republic of Bulgaria, another Member State of the EU or a State party to the Agreement on the EEA can be postal operators (Art.18). Art. 39 of the Postal Services Act enables the CRC to grant an “individual licence” for the handling of postal money orders.

4. The LPSPS regulates the licensing of payment institutions (Art. 7) and the licensing of electronic money institutions (Art. 36(1)).³ 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, see R.26.

5. **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.

6. 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 (approximately EUR 2 500) for a natural person to BGN 80 000 (approximately EUR 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 (approximately EUR 2 500 to EUR 5 000) and court ordered property confiscation. The maximum penalty may be applied in cases where “consideration damages” have been caused or “considerable

3. 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.

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.

7. 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.

8. Regarding the handling of postal money orders, the CRC investigates unlicensed persons on the basis of information provided through consumer complaints, whistle-blowers, competitors or competent authorities. According to Art. 99(1) of the Postal Services Act (amended by SG 84/2023) whoever, without a license, provides services under Art. 39 shall be liable to a fine of BGN 10 000 to BGN 20 000 (approximately EUR 5 000 to EUR 10 000). According to Art. 99(5) of the Postal Services Act (amended by SG 84/2023) a proprietary sanction of BGN 15 000 to BGN 25 000 (approximately EUR 7 500 to EUR 12 500) is imposed on a legal entity or a sole trader who continues to provide services after the termination or revocation of their individual licence.

9. **Criterion 14.3** – According to Art. 108 of the LMML and Art. 14a of the LMFT as well as Art. 32(e)(1) and Art. 32(e)(7)(18) of the Rules on Implementation of the Law on State Agency for National Security (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 postal⁴ money remittance service providers.

10. Art. 108 of the LMML and Art. 14a of the LMFT as well as Art. 79 of the Law on Credit Institutions (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 service providers to exercise supervisory powers for AML/CFT purposes. For more information please also see R.26 and R.27.

11. **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.

12. 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). According to Art. 20 (12), postal operators are obliged to keep and maintain an up-to-date list of all access points (this includes its agents).

13. **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. There is also an explicit requirement placed on the payment service provider to include their agents in the AML/CFT programmes and monitor for compliance with these programmes (Art. 101(19) of LMML (amended by SG 84/2023)).

Weighting and Conclusion

14. **R.14 is re-rated compliant.**

4. 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.

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, no upgrade)

1. In the 2022 MER, Bulgaria was rated PC on R.15. The assessment identified some technical deficiencies related to assessment of the risk of new technologies; coverage of the virtual assets service providers (VASP) activities; application of fit and proper measures; application of preventative measures by VASPs; application of measures related to implementation of TF and PF-related TFS; and international cooperation.

2. During the follow-up period Bulgaria ensured that all the VASP activities and operations defined by the FATF Standards are regulated (LMML, Art. 4 (38 and 39)).

3. **Criterion 15.1 –**

Country level

4. At a national level, Art. 96(1)(2) of the LMML (amended by SG No. 84/2023) provides a requirement for conducting and updating an assessment of the potential ML/TF risks arising from the introduction of new products, business practices and delivery mechanisms, as well as the use of new technologies in new or pre-existing products, business practices and delivery mechanisms. Bulgaria has taken steps to analyse new technologies-related risks during its 2023 NRA exercise. The analysis is covered under specific topics, rather than as a holistic risk assessment on the topic, which is considered to be a minor shortcoming. For example, it is covered in: (i) Chapter 3 - subsections Frauds, Including Investment and Computer Frauds, drug trafficking, Assisting the Process of Money Laundering and “Professional Launderers” and National Money Laundering and Terrorist Financing Vulnerabilities; (ii) Chapter 5 - ML risk assessment by economic sectors, subsection on information technology (IT) and electronic money; (iii) Chapter 6 - ML risk assessment in financial sector and DFNBPs sector and subsection on e-money; (iv) Chapter 7- Cross-border risks; and (v) Chapter 8 – TF risks assessment. This, however, does not explicitly cover analysis of the ML/TF risks related to the use of developing technology.

Obligated entities level

5. Under Art. 48a(1) of the LMML (amended by SG No. 84/2023), 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. This does not explicitly cover the use of developing technology.

6. **Criterion 15.2 –**

- (a) Art. 48a(2) of the LMML (amended by SG No. 84/2023) 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.
- (b) Apart from the general requirement to mitigate risks (LMML. Art. 101(2)(8)), there is no explicit requirement to take appropriate measures to manage and mitigate the risks that specifically target new products and new business practices, new delivery mechanisms or new and developing technologies. However, this shortcoming is partly mitigated by: (i) the requirement under Art. 35(5) of the LMML, according to which OEs have to take enhanced measures where new technologies-related risks are assessed as high as part of the NRA or business risk assessment (BRA) process or based on the results of the OE's internal ML/TF

risk assessment; and (ii) 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.

9. Criterion 15.3 –

- (a) In February 2023 Bulgaria completed a Sectoral assessment of ML/TF risks related to VAs and VASPs which constitutes a comprehensive analysis of ML/TF threats, vulnerabilities, inherent risk factors associated with VA/VASPs based on the following components: (i) review of contextual factors affecting the VA ecosystem; (ii) measurement of the materiality of the VA and VASP sector in Bulgaria, including products and services involving VAs and VASPs in non-VASP regulated sectors (such as financial institutions and designated non-financial businesses and professions (DNFBPs)); (iii) analysis of the regulation and legal framework relevant to VAs/VASPs; (iv) review of the supervisory practice by FID-SANS; (v) analysis of the threats stemming from predicate offences, which serve as the main source for generating criminal proceeds for the VA ecosystem, as well as TF threat analysis; (vi) vulnerability analysis from legislative, operational and risk awareness perspective; (vii) analysis of customers and user profiles involved in VA and VASP-related crimes; (viii) analysis of other (non-VASP) economic sectors involved in the use of VAs; and (ix) analysis of VAs products and VASPs services. The findings from each of these components were cross-analysed and integrated to produce a matrix or risk scenarios for Bulgaria in four risk assessment sections.
- (b) Art. 96 and Art. 97 of LMML and Art. 59 of RILMML requires that at the national level the results of the NRA which also include assessment of risks related to VASPs and VAs be used to mitigate the identified risks.

Bulgaria adopted a strategy for countering ML and TF (2023-2027) which among others establishes priorities and defines key actions based on: (i) the 2023 NRA; (ii) Sectoral Assessment of ML/TF risks related to VAs and VASPs (February 2023). One of the main purposes of the Strategy is to properly allocate resources to areas where higher ML/TF risks are identified.

The Action Plan for the implementation of the Strategy was approved on 23 November 2023 by the Council for Coordination and Cooperation and subsequently adopted by the Council of Ministers (Council of Ministers Decision No. 66 of 31 January 2024).

- (c) VASPs are required to identify, assess, manage and mitigate risks in line with the requirements analysed under c.1.10 and c.1.11.

10. Criterion 15.4 –

- (a) The scope of the covered VASPs is aligned with the FATF definition (Art. 4(38-39) and paragraph 1(30-31) of the LMML (amended by SG No. 84/2023)). This criterion is addressed through Art. 9a of LMML on registration of VASPs. The registration requirements are equally applicable to legal and natural persons who provide VASP services by way of business inside or outside Bulgaria (and so applies to all legal persons created in Bulgaria). The VASPs registry is maintained by the National Revenue Agency.
- (b) There are legal provisions in Art. 9d of the LMML (amended by SG No. 84/2023) that prohibit criminals from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP. However, LMML does not prescribe such requirements for criminals' associates.

11. Criterion 15.5 – Art. 116a of LMML prescribes appropriate sanctions for VASPs that provide services without being entered into the register referred under Art. 9a. The fines are applicable to both natural and legal persons, whereby the fines amount.

12. For natural persons: (i) a fine of BGN 2 000 (approximately EUR 1 000) - BGN 10 000 (approximately EUR 5 100); (ii) a fine of BGN 4 000 (approximately EUR 2 000) - BGN 20 000

(approximately EUR 10 200) upon a repeated violation; and (iii) a fine of BGN 5 000 (approximately EUR 2 600) - BGN 50 000 (approximately EUR 25 600) for serious or systematic violations.

13. For legal persons: (i) a fine of BGN 5 000 (approximately EUR 2 600) - BGN 50 000 (approximately EUR 25 600); (ii) a fine of BGN 10 000 (approximately EUR 5 100) - BGN 100 000 (approximately EUR 51 200) upon a repeated violation; and (iii) a fine of BGN 50 000 (EUR 25 600) - BGN 500 000 (approximately EUR 260 000) for serious or systematic violations.

14. The range of fines that is available can be applied proportionately to greater or lesser breaches of requirements.

15. Written statements ascertaining violations of registration requirements under Art. 116a of LMML must be drawn up, and penalty decrees are issued by the Executive Director of the National Revenue Agency (Art. 4(38)(39) (LMML, Art. 123(3)). On the basis of its internal procedures, the National Revenue Agency takes action on a report from a person, institution or other administration, containing information about violations committed by obliged persons of legal acts for which the National Revenue Agency is the competent authority (such as the LMML and LMFT) (Procedure for Conducting Proceedings on Signals for Violations of the Regulatory Acts, Control of for which the National Revenue Agency is the Competent Authority to Exercise Control over the Implementation, 2022 NK43).

16. However, there are no proactive actions taken by the authorities to identify natural or legal persons carrying on VASP activities without a prior registration.

17. **Criterion 15.6 –**

- (a) VASPs are subject to AML/CFT requirements and are supervised by FID-SANS (Art.108 of the LMML and Art. 14a of the LMFT). The provisions of Art. 114 of the LMML (SG No. 84/2023) provide a legal basis for a risk-based supervision of VASPs. Relevant risk factors, characteristics of the OE or group and information collected by FID-SANS to assess and understand the ML/TF risk the OE is exposed to are used for planning supervisory activities, including making decisions on the scope, depth, duration and frequency of the on-site inspections proportionate to those risks. In addition, Art. 115(3) of LMML prescribes that the results of the NRA shall be taken into consideration when applying the risk-based approach to supervision. Ongoing monitoring and periodic reviews of risk assessments, including upon the occurrence of essential circumstances or changes in the OE management and activities (to ensure that the risk assessment and resource allocation are current, applicable and relevant) are required by Art. 114, paragraph 1, item 4 of LMML.

FID-SANS has internal manuals in place for carrying out on-site and off-site inspections, whereby inspections are carried by taking into account (inter alia): (i) NRA; (ii) sectoral risk assessment related to VAs and VASPs; and (iii) FID-SANS data on the number of received STRs and their quality by sectors. The risk of individual OE is evaluated by FID-SANS during the off-site monitoring process, based on the collected information.

FID-SANS conducts two types of inspections. Off-site inspections (or so-called remote checks) include reviews of internal documents, rules, policies, own risk assessment and matrix of the inspected OE. On-site inspections are conducted based on the scope outlined in the inspection plan. Follow-up actions are also carried out, whereby the inspected OE is requested to develop and provide to FID-SANS an action plan for addressing the identified deficiencies, if there are any.

- (b) FID-SANS is authorised to carry out on-site and off-site inspections of VASPs (see c.15.6(a)) regarding the application of AML/CFT requirements. Compulsion of information is required by Art. 109 of the LMML and Art. 14a of the LMFT.

FID-SANS has powers to: (i) apply remediation measures such as ordering a VASP to cease a violation, to take specific measures necessary for remedying the violation and set a time limit for taking such measures (Art. 126 of LMML and Art. 14a of LMFT ; (ii) impose sanctions on

VASPs, their managers and representatives for AML/CFT breaches (Art. 123(1) of LMML and Art. 16(1) of LMFT); (iii) in case of serious or systematic violations, forbid a natural person from holding a senior management position (Art. 124 of LMML and Art. 15(7) of LMFT); and (iv) 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, to withdraw authorisations for licence or registration. Equivalent provisions are at Art. 15(8) of the LMFT. However, there are no legal provisions enabling restriction or suspension of a VASP's registration.

18. **Criterion 15.7** – No specific AML/CFT guidelines and feedback have been issued for VASPs. In 2023 FID-SANS issued new guidances (Guidance on Measures against TF, Guidelines related to customer risk assessments, and Guidelines related to PEPs) which are relevant to all OEs, including VASPs. However, there were no guidelines provided by the authorities to VASPs to assist them in detecting and reporting suspicious transactions. The shortcomings identified under R.34 also apply here.

19. **Criterion 15.8** –

- (a) Shortcomings identified under R.35 (c.35.1) apply here.
- (b) Sanctions are applicable to directors and senior management (c.35.2).

20. **Criterion 15.9** – Shortcomings under Recommendations 10, 13, 16 and 20 apply here. When weighting the shortcomings, the risk and materiality of the VASP sector is taken into consideration.

- (a) According to Art. 11(5) of LMML, for the occasional transactions (i.e., an exchange between VAs and fiat currencies, exchange or transfer of VAs) the designated threshold where CDD is applicable for VASPs amounts to or exceeds the BGN equivalent of EUR 1 000 or the equivalent in another currency.
- (b) The EU Regulation (EU) 2015/847 which provides the legal basis for compliance under the R.16 is not applicable to VASPs. No other requirements are in place.

21. **Criterion 15.10** – With respect to targeted financial sanctions (TFS), mechanisms explained under R.6 and R.7 apply to VASPs. With respect to c.6.6.(g) Art. 5(b) of the LMFT (amended by SG No. 84/2023) prescribes that competent authorities shall issue guidance for implementing TFS measures as well as the conditions for suspension. On this basis, the authorities have issued and published “Guidance on implementation of the measures against financing of terrorism” (2023). Shortcomings identified at R.7 apply here, namely at sub-criteria c.7.2(e), c.7.4(d) and 7.3.

22. **Criterion 15.11** – The analysis under R.37 to R.40 is also valid under this criterion. A partial progress was demonstrated with: (i) R.5, which rectified some of the deficiencies by virtue of adoption of amendments to Penal Code, those having a cascading effect on c.37.7 and c.39.1(a), (ii) c.37.2 which rectified the deficiency with the timely mutual legal assistance (MLA) co-operation with non-EU counterparts; and (iii) c.40.15-40.16 which rectified the remaining issues with FID-SANS powers for international co-operation as a VASP supervisor.

Weighting and Conclusion

23. The following shortcomings have been identified: (i) the lack of holistic risk assessment by the country when analysing new technologies-related risks, which also not explicitly covers the use of developing technology (c.15.1);(ii) apart from the 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 products and new business practices, new delivery mechanisms (c.15.2(b)); (iii) there are no legal provisions that would prevent criminals' associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP(c.15.4(b)); (iv) no proactive actions taken by the authorities to identify natural or legal persons carrying on VASP activities without a prior registration (c.15.5); (v) there are no legal provisions enabling restriction or suspension of a VASP's registration (c.15.6(b)); (vi) no VASP specific AML/CFT guideline is issued (c.15.7); (vii) shortcomings identified under R. 7, (c.7.2(e), 7.3, c.7.4(d)), 10, 13, 16, 20,34, 35, R.37 – R.40 apply to VASPs. Cumulatively these are considered moderate deficiencies in light of the growing materiality of the sector. **R.15 remains rated partially compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.18. The assessment identified some technical deficiencies related to requirement to have policies and procedures on employee screening; requirement for internal AML/CFT audit function; compliance with AML/CFT requirements via group-wide procedures; data and information exchange between group entities; application of AML/CFT measures consistent with the home country requirements.

2. **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.

Compliance management arrangements

3. 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.

4. 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.

5. 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).

Employee screening

6. There is a requirement in the LMML for OEs to have internal screening procedures to ensure high standards when hiring employees (Art. 101(2) (13-14) of the LMML (amended by SG No. 60/2023)).

Ongoing training

7. 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.

Independent audit function

8. Art. 101(2) (3-4) of the LMML requires the OEs to establish rules which shall contain the procedure to carry out a review, verification and assessment of the AML/CFT rules, procedures and requirements by the internal control over the fulfilment of the AML/CFT obligations. However, the limitation following the wording of the legislation, i.e., “possibility of conducting an independent audit to test and evaluate compliance, where appropriate with regard to the size and nature of the business” (101(2)(5) remains. Hence it does not seem that the requirement for an audit is mandatory.

9. 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 European Banking Authority (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 explicitly refer to AML/CFT audit.

10. **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 (Amended, SG No. 84/2023).

11. 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.

Information sharing

12. 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.

Provision of AML/CFT information by group-level functions

13. Art. 80(3) LMML permits disclosure of AML/CFT related data and information to all types of FIs that are part of the same group (Supplemented, SG No. 84/2023). Within the context of Bulgaria postal undertakings do not belong to financial groups, hence these provisions of 18(2(b)) are not applicable to them.

14. 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. There is also an explicit requirement to share information regarding unusual activity and/or its analysis (Art.101(2)(18) of the LMML (amended by SG No. 84/2023))

Safeguards

15. 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. In addition, there are adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off (Art.101(2) (18)(e) of the LMML).

16. **Criterion 18.3** – Art. 7(1-2) of the LMML requires OEs to ensure the effective application of measures by branches and subsidiaries in foreign countries, including the sharing of information, in so far as is permitted under the legislation of the country. Where the legislation of a 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. The requirements under Art. 7(1) of the LMML are applicable also to foreign branches and majority owned subsidiaries located in the EU countries (amended by SG No. 84/2023).

17. 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 (Article 7(1) of the LMML (amended by SG No. 84/2023), and explicitly covers a scenario where AML/CFT requirements of the host country are less strict than those of the home country.

Weighting and Conclusion

18. Bulgaria meets most of the requirements, but deficiency with respect to mandatory audit function remains (c.18.1(d)). **R. 18 is re-rated largely compliant.**

Recommendation 22 – DNFBPs: Customer due diligence

	Year	Rating
MER	2022	PC
FUR1	2024	↑ LC upgrade requested

1. In the 2022 MER, Bulgaria was rated PC with R.12. The assessment identified some technical deficiencies related to implementation of measures under R.10, R.11, R.12, and R.15 which were also relevant to DNFBPs.

2. 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.

3. **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 requirements at Art. 11 (6-7) of the LMML applies (amended by SG No. 84/2023).

Casinos

4. 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.

Real estate agents

5. 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.

Dealers in precious metals and stones

6. 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 Limitation of Cash Payments Act 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.

Lawyers, notaries, other independent legal professional and accountants

7. Listed at item 15 of Art. 4 of 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.

Trust and company service providers.

8. Listed at item 16 of Art. 4 of 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.

9. The deficiencies identified under R.10 (c.10.9, 10.10 and 10.16) also apply to DNFBPs.

10. **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.

11. **Criterion 22.3** – Reference is made to the analysis for R.12 (c.12.1-12.3) on the general coverage of PEP requirements within Bulgarian legislation, which are equally applicable to DNFBPs. The legal framework set for c.12.4 under Art. 43 of the LMML is not applicable to DNFBPs.

12. **Criterion 22.4** – Reference is made to the analysis for R.15 (c.15.1-15.2), which is equally applicable to DNFBPs.

13. **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

14. Some minor deficiencies remain under R.10 and R.15 which are relevant to DNFBPs. **R.22 is re-rated largely compliant.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

	Year	Rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.25. The assessment identified some technical deficiencies related to requirement to disclose the status to FIs/DNFBPs; powers of competent authorities to obtain beneficial ownership information on behalf of foreign counterparts; and sanctions applicable to trustees.

2. Criterion 25.1 –

- (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) 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.

3. 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.

4. **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 paragraph 2 (1) p.2 of the LMML shall apply.

5. 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.

6. 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.

7. The definition of Beneficial owner in respect of Trusts is contained in paragraph 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.

8. 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.

9. **Criterion 25.3** – There is an obligation for trustees to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction (LMML, Art.62(2)).

10. **Criterion 25.4** – Trustees are not prevented by law or other enforceable means from providing competent authorities with any information relating to the trust.

11. **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 paragraph 2(1)(2) of the LMML shall apply. There is a legal mechanism in place to identify those who are conducting trustee services (LMML, Art.123(3); BULSTAT Register Act, Art. 3(3), and Art. 12(1); and Internal Rules for Establishing Administrative Violations and Imposing Administrative Penalties (Art. 4 -6)).

12. **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 suspicious transaction report (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.

The Financial Supervision Commission (FSC) has powers under Art. 13(1)(23-26) and Art. 25(4)-(6) of the Law on the Financial Supervision Commission (FSCA) in respect of international co-operation. Art. 257 and 262(2)(1) of the Markets in Financial Instruments Act (MFIA) allows the provision by the FSC of information to competent authorities of EU member states. Art. 258 of the Collective Investment Schemes and Other Undertakings for Collective Investments Act (CISOUCIA) allows the provision by the FSC of information to

competent authorities of EU member states. Art. 100z(1) and (3) of the Public Offering of Securities Act 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 Prosecutor's office may obtain any information by the means referred in c.24.10 on legal arrangements, including beneficial ownership for the provision of foreign states.

13. **Criterion 25.7** – Trustees as OEs under the LMML are subject to sanctions analysed at R.35. Shortcomings identified at R.35 apply here.

14. In addition, Art. 40 of the Act on the Commercial Register and the Non-Profit Legal Entities Register 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 proportionate and dissuasive (range BGN 1000 – BGN 10 000, approximately EUR 500 – EUR 5000).

15. **Criterion 25.8** – Obligated entities should grant to competent authorities timely access to information regarding the trust (LMML, Art.72, 74 and 110). Administrative sanctions for breaches of this obligation are set in the LMML (Art. 116 and 118) range from BGN 1 000 (approximately EUR 500) for the first violation, up to BGN 2 000 000 (approximately EUR 1 000 000) or up to double amount of the benefit derived from the violation if the said benefit can be identified. For non-professional trustees those obligations are set in the Law on SANS (Art. 129) and the Ministry of Interior Act (Art. 4.). Sanctions for breaches of this obligation are set in the Law on SANS (Art. 134) ranging from BGN 500 (approximately EUR 250) to BGN 2000 (approximately EUR 1000) and similar fines are also set in the Ministry of Interior Act (Art.257). These sanctions set for failing to grant to competent authorities with timely access to information regarding the trust referred to in criterion 25.1 are considered proportionate and dissuasive.

Weighting and Conclusion

16. The following deficiencies apply: (i) professional trustees of foreign law trusts 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; (ii) the range of sanctions applicable to trustees for failure to meet their AML/CFT obligations is not always considered to be proportionate. **R.25 is re-rated largely compliant.**

Recommendation 26 – Regulation and supervision of financial institutions

	Year	Rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.26. The assessment identified following technical deficiencies: (i) Supervisors were not explicitly required to assess the ML/TF risk profile of an individual financial institution or group, including the risk of noncompliance (c.26.6); (ii) Entry controls of all FIs did not explicitly prevent licensing/registration in case of association with criminals; (iii) Some financial services fell 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); (iv) Number of various other shortcomings established in licensing requirements related to the absence of explicit requirements regarding non-criminality, as well as rehabilitation, etc. (c.26.3); (v) there was 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 was 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); (vi) It was 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; (vii) Regulation and supervision of FIs (that fall outside the scope of core principles institutions and PIs/EMIs) demonstrated notable shortcomings and did not appear to have regard to the ML/TF risks; (viii) Regulation and supervision of currency exchange providers by the NaRA and postal money operators by the CRC was not risk based and systems for supervisory monitoring were underdeveloped (c.26.4).

2. **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.

3. Further, Art. 108(6) of the LMML establishes that control of compliance with some provisions under LMML shall be exercised using a risk-based approach by the BNB, the FSC and CRC (over the PMOs). This includes both, off-site and onsite supervision. Art. 14a(2)(3) 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.

4. 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.

5. 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 paragraph1(11)) means the State bodies empowered by a law or another statutory instrument act to exercise general supervision over the activities of OEs. Such other supervisory authority is the National Revenue Agency (NaRA) regarding currency exchange (Currency Law, Art. 16(4); LMML, Art.108(7)) (see Immediate Outcome (IO) 3 for more information).

6. **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 CISOUICIA; insurance operators and intermediaries under Articles 28 and 296 of the Insurance Code (IC).

7. 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 of August 8, 2003 on the terms and conditions for entry in the register and the requirements for the activity of exchange bureaus. The LMML also provides for the requirement for a legal person which provides by way of business access to safe deposit boxes in public vaults to register within Ministry of Interior (MoI). 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.

8. **Criterion 26.3** – FIs are subject to varying levels of entry controls under the relevant legislation, as set out below. The legal requirements or regulatory measures explicitly prevent licensing where relevant individuals are associated to criminals, with some minor exceptions as explained below.

9. 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 Social Insurance Code (SIC), crimes of negligence are not a barrier to entry. It is the Assessment Team (AT’s) view that rehabilitation is easily achievable, however this is considered to be a minor shortcoming.

10. Art 108(8) LMML requires FID-SANS to carry out offsite inspections regarding requirements under Art. 9d 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, trust and company service provider or real estate agent.

11. 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.

12. 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.

13. License/approval can be refused in cases where the links with close associates give grounds for concern regarding the reputation and integrity of the applicant (LCI, Art. 11, 14, 15(1)2 and 28a(2); BNB Ordinance 20, Art. 21, 22; BNB Ordinance 2, Art. 33g and 33h). This includes associates to criminals.

14. The BNB and the European Central Bank (ECB) co-operation 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.⁵

15. Regarding acquisitions of shareholdings, Art. 28(1) of the LCI establishes that prior written approval of the BNB is required to acquire, directly or indirectly, a qualifying shareholding Art. 28a(3)

5. The ECB is in charge of the authorisation (licensing) procedures in Bulgaria, after establishing a close co-operation mechanism with the BNB.

requires BNB assessment of the application with a view to ensuring its future sound and reasonable management, including consideration of the reputation of the applicant as well as ML/TF risk.

16. Securities: 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, which includes absence of a conviction for a premeditated offence at public law for the applicant, as well as ML/TF risk, and the reliability and suitability of close associates (MFIA, Art 13(4)8)).

17. Collective investment schemes: FSC licensing prohibits, under Art. 10 of the CISOU CIA, 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”.

18. Art. 224(1) of the CISOU CIA 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. This also includes their associates (CISOU CIA, Art 93, paragraph 1, item 11).

19. 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.

20. Pension insurance: Art. 121g(3) of the SIC prohibits any person from acquiring, either directly or indirectly, a qualifying shareholding without prior FSC approval. 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, agents and their close associates “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”.

21. 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”. Pursuant to the Art. 10(4)(12) of the LPSPS the persons managing and representing the applicant company and the members of its management and supervision bodies, including the representatives of legal entities and the persons holding, directly or indirectly, qualifying holdings in the applicant’s capital within the meaning of Article 4(1), point 36 of Regulation (EU) No 575/2013, which is 10 per cent, shall not give grounds to doubt their good reputation to comply with the licensing obligations. 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. The approval shall be granted taking into account the assessment of the reputation of the applicant and his close associates according to the Art. 14 (5) (1) of the LPSPS. According to the definition in additional provisions, p. 68. of the LPSPS “Close associate” includes persons who are close business partners and family members/spouses of the beneficial owners, persons with a direct qualifying holding and persons managing and representing the PI/EMI.

22. 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 a person with a qualifying holding must provide information regarding probity, including a 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 premeditated crime of general nature, unless rehabilitated.

23. 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.

24. Postal operators handling postal money orders (PMO): Chapter Five of the Postal Services Act details the licensing procedure. Under Article 47(2)(4) of the Postal Service Act, the CRC shall refuse to grant a licence if natural persons who are members of the governing body or beneficial owners of the applicant have been convicted for crimes of a general nature, unless they have been rehabilitated or pardoned. Similar provisions exist for legal persons. Associates are not covered. However, this is considered to be a minor deficiency.

Other FIs

25. 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. 3a 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.

26. **Criterion 26.4 –**

Basel Committee on Banking Supervision (BCBS) Principles

27. The International Monetary Fund (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

28. 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

29. Authorities reported that the assessment was recently carried out by European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA) of the independence of national competent authorities, including Bulgaria. The resulting EBA, EIOPA and ESMA reports provide aggregated results rather than country-specific results.

30. Based on the additional information that was made available to the assessment team (AT) by the authorities, supervision is mostly in line with applicable core principles.

Other financial institutions

31. 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) also considers the ML/TF risks in these sectors (“BNB AML-CFT Rules and Procedures of SOPS Unit” (Chapter Two, Part One) and the requirements in “BNB-MFM_FID-SANS Methodology for joint supervision”).

32. Regulation and supervision of currency exchange providers by the NaRA and postal money operators by the CRC is based on the ML/TF risks in that sector (LMML (Art. 114)).

33. **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.

34. According to Article 114 (1), items 1- 3 of the LMML, the supervisory authorities, when implementing a risk-based approach to supervision, base the frequency and intensity of on-site supervision and control activities on the risk profile of obliged entities. Whilst the above addresses sub-criteria 26.5(a) and 26.5(b), it does not explicitly cover sub-criterion (c). The absence of compliance with c.26.5(c) is a moderate 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.

35. 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.

36. The BNB (for banks and PIs/EMIs), FSC (for securities and insurance), the CRC (for postal operators) 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.

37. **Criterion 26.6** – Art. 114(1), items 1 and 4 of the LMML require 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 the Banking Supervision Department of the Bulgaria National Bank (BNB-SSAD's) Operational Rules and Procedures.

Weighting and Conclusion

38. Following shortcomings remain: (i) Entry controls for some FIs do not explicitly prevent licensing/registration in case of association with criminals, in particular: (a) associates of criminals are not covered for PMOs (minor shortcoming); and (b) entry controls do not extend to BOs of currency exchange offices or managers of insurance operators and intermediaries (moderate shortcoming) (c.26.3). (ii) There is no explicit requirement to determine the frequency and intensity of supervision based on characteristics of FIs and financial groups, including the diversity and number (c.26.5(c)) (moderate shortcoming). (iii) 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 (minor shortcoming) (c.26.6). Although few moderately weighted shortcomings exist, overall compliance with this Recommendation is largely compliant. Consequently, **R.26 is re-rated largely compliant.**

Recommendation 27 – Powers of supervisors

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ LC (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.27. The assessment identified following technical deficiencies: (i) The legal basis for supervision, incl. on-site inspections by NaRA (regarding currency exchange) and CRC (regarding postal operators) was not explicitly established (c. 27.2); (ii) LMFT did 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 were not available in all cases (c. 27.4).

2. **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.

3. Art. 108(6) of the LMML establishes that control of compliance with some provisions under LMML shall be exercised using a risk-based approach by the BNB, FSC and the CRC. This includes both, off-site and onsite supervision.

4. 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.

5. Art. 115(4) of the LMML requires the control authorities to co-operate and exchange information with each other.

6. Further, RILSANS requires that FID-SANS receive, store, examine, analyse and disclose information collected regarding OEs compliance with the LMML, LMFT, Law on State Agency for National Security (LSANS) and Acts regarding their implementation such as RILMML.

7. **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 and terrorism financing, as well as whenever there is a suspicion of money laundering or terrorism financing (LMML, Chapter 9, including Art.108 and LMFT, Art.14a(2)). 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 shall be exercised using a risk-based approach by the BNB, FSC and CRC (regarding postal operators and their representatives). This includes both, off-site and onsite supervision.

8. For TFS related to TF supervision please refer to c.27.1.

9. **Criterion 27.3** – Art. 109 of the LMML provides FID-SANS and other supervisory authorities (the BNB, FSC and CRC (regarding postal operators and their representatives)) 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.

10. Regarding compulsion of information regarding compliance with LMFT (on TF and TFS), Art. 14a(2) and (3) of the LMFT states that control shall be conducted by FID-SANS and other supervisory authorities (the BNB, FSC and CRC (regarding postal operators and their representatives) in accordance with the procedures established under the LMML, including the inspections powers detailed above, thus having the same powers to compel information required to verify compliance with the LMFT as with the LMML.

11. **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, in particular: monetary penalties applicable to directors and senior management are not fully dissuasive and 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.

Weighting and Conclusion

12. Deficiencies exist in the range of sanctions that are available to supervisors. Although moderately weighted shortcoming in relation to c.27.4 exist, overall compliance with this Recommendation amounts to largely compliant. Consequently, **R.27 is re-rated largely compliant.**

Recommendation 32 – Cash Couriers

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ C (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.32. The assessment identified following technical deficiencies: (i) The criminal sanctioning regime was incomplete as it only exists for large-scale cases of noncompliance at the external EU borders. Temporarily retainment of cash in the sense of c.32.8 was only formally provided at the EU external borders, but domestic legislation for the practical application of this mechanism was still not in place, while there was no such mechanism at all for the EU internal borders, as a result of which there were no legal powers for the detention of cash suspected to be linked to ML/TF.

2. **Criterion 32.1** – For incoming and outgoing cross-border transportation of cash and Bearer-negotiable instruments (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. 11a of the Currency Act.

3. 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 (2018 EU Regulation) entered in force on 3 June 2021 and has since been directly applicable. The Currency Act is harmonised with the 2018 EU Regulation with last amendments made to Currency Act (amendments made with SG No. 82/29.09.2023). Cash definition under the 2018 EU Regulation covers also BNIs (2018 EU Regulation, Art. 2, paragraph 1, letter a) and Art. 2, paragraph 1, letter d)) and the Currency Act makes relevant references to 2018 EU Regulation (Supplementary Provisions, paragraph1, points 6 and 7).

4. The transfer of cash across the country's border by postal and/or courier shipments is prohibited, except for shipments with a declared value (Currency Act, Art. 10c(1)). Disclosure system applies when transporting unaccompanied cash in the amount of EUR 10 000 or more or its equivalent in BGN both at external and internal borders of EU (Currency Act, Art.10c(2) and (3)).

5. **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. 10a 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 (Currency Act, Art.11a (2)).

6. 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.

7. **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 (Currency Act, Art. 10b (2)) using the relevant declaration form (Currency Act, Art.11a(3)).

8. **Criterion 32.4** – 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.

9. A protocol is drawn up for the control of cash, and the cash is detained with a receipt under Art. 15, para. 2, item 9 of the Customs Act (Currency Act, Art. 16(1), (2) and (3)). The customs authorities may require proof of ownership, economic provenance of the cash and its intended use (Currency Act, Art.11(2)).

10. **Criterion 32.5** – Persons who make a false declaration or disclosure are subject to a sufficient range of criminal and administrative sanctions that can be applied proportionately to greater and lesser breaches of requirements and are dissuasive. Failure to comply with the obligation to declare/disclose cash can be sanctioned under the Currency Act or under the Criminal Code depending on the amount of the non-declared cash as follows:

11. Failure to declare or disclose cash, refusal to declare, providing incorrect or incomplete information (i.e. false declaration/disclosure) or failing to make cash available to the customs authorities for the purpose of conducting a control are administrative offences and punishable by a fine, where not a criminal offence. An administrative fine in the amount of 20% of the value of the undeclared cash may be applied, and, in the case of concealing cash, the penalty increases to 25% of the value of the undeclared cash (Currency Act, Art. 10a (2) and (3); Art. 10b (2) and (3); Art. 10c (2), (3) and (5); and Art.18 (2) and [3]). In case of repeated violation, fines may be applied up to 25% and 33% respectively (Currency Act, Art. 18 (7), p. 3 and 4)). The administrative sanctions are the same for accompanied and unaccompanied cash, as well as for cash carried across the EU external and EU internal borders.

12. If the value of non-declared or non-disclosed cash found is under the threshold of “*particularly large amount*” (currently EUR 66 785⁶), the offender is sanctioned under the Currency Act as described above. If the value of the cash found is at or over EUR 66 785, failure to fulfil the obligation to declare cash (including false declaration/disclosure) carried across the country’s border shall be punished by imprisonment for up to five years and a fine in the amount of 20% of the value of the undeclared cash (Criminal Code, Art. 251 (1)). Sanctions under Criminal Code are applied at EU external and internal borders in case of false declaration or disclosure.

13. **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.

14. 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.

15. 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 (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.

6. The amount is tied to minimum salary in Bulgaria.

16. **Criterion 32.7** – Instructions for cooperation between Customs authorities and Ministry of Interior (MoI) as well as the National Revenue Agency (NaRA) 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 NaRA 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.

17. **Criterion 32.8** – Art. 7 of the EU Regulation 2018/1672 provides that the competent authorities may temporarily detain cash (including BNIs) for up to 30 days in order to ascertain whether evidence of ML/TF may be found in cases 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. Same is stipulated in the Art.11(1) of the Currency Act, which includes also that the obligation to declare or to disclose is not fulfilled if the declared/disclosed information is incorrect or incomplete (i.e. false declaration/disclosure).

18. **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.

19. 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).

20. The retention period for cash declarations generally is 5 years pursuant to Art. 11a(4) 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.

21. **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. 11a (6) 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.

22. **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

23. All criteria are met. **R.32 is re-rated C.**

Recommendation 33 – Statistics

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	↑ C (upgrade requested)

1. In the 2022 MER, Bulgaria was rated PC on R.32. The assessment identified that although legal requirements to comply with c.33.1 are in place, the country only kept 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 was a major manual work for the country. Therefore, the AT could not conclude that Bulgaria maintained comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system. The country was encouraged to keep more detailed statistics.

2. **Criterion 33.1** – In accordance with Art. 71(1), (2) and (6) of the LMML competent authorities shall maintain statistics on matters relevant to the effectiveness and efficiency of the systems to prevent and combat ML/TF. This includes:

- (a) *STRs received and disseminated* – Authorities maintain the statistics on 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, which include STRs received and disseminated. In practice, this is achieved through the FID-SANS case management procedures, which ensure gathering relevant statistics by FIU, including breakdown by different criteria (e.g. predicate offences indicated in STRs).
- (b) *ML/TF Investigations, Prosecutions and Convictions* – Authorities maintain the statistics on ML/TF investigations, prosecutions and convictions based on the Rules for the Collection and Completion of the Data in the National Money Laundering and Terrorist Financing Risk Assessment Register, approved by Order No. RD-02-14 of July 10, 2023 of the Prosecutor General (Order on the Register of NRA). Relevant data is entered (as of January 1, 2022) to the Unified Information System of PRB (Register of NRA), which allows the data to be automatically displayed and cross-analysed. The data is updated by the supervising prosecutor when the case is brought to court as well as when a judgment comes into force. Pursuant to Art. 71(2) item 2 and Art. 71(6) of the LMML, statistical data shall include data measuring the pre-investigation, investigation and judicial phases of cases of ML/FT. In particular, these statistics must include: (i) the number of checks conducted by the Law Enforcement Agencies (LEAs) on an annual basis; (ii) the number of cases investigated on an annual basis; (iii) the number of persons against whom criminal proceedings are instituted; (iv) the number of persons convicted for ML or TF; and (v) the types of predicate offences.
- (c) *Property frozen, seized and confiscated* – Authorities maintain the statistics on property frozen, seized and confiscated. Pursuant to Art. 71(2) item 2 and Art. 71(6) of the LMML and the Order on the Register of NRA the relevant authorities (prosecutor’s offices) must collect relevant data to the Register of NRA, which includes data on: (i) property that was secured (seized/frozen) during the investigation phase, including abroad and its value/type (if at the stage of entering the data, its value is not established, its type is noted, e.g. apartment, vehicle, etc.); (ii) the property confiscated with a final judgment; and (iii) data on the predicate crime. In each of the above-mentioned sub-registers, data on the predicate crime is collected, and the format of the sub-registers allows, by selecting a crime from a list in a drop-down menu, data on the secured and respectively confiscated property, to be found.

In addition, the CACIAF administers a register of seized assets (electronic database) on the basis of Art. 170, paragraph 1 of Illegal Asset Forfeiture Act (IAFA) which includes data identifying the specific seized assets on which security measures (seizure/freezing) have been imposed, information on initiated proceedings by the CACIAF for confiscation of illegally acquired property, namely on: (i) persons against whom proceedings have been initiated and

third parties related to them; (ii) data from judicial authorities on the collateral proceedings and the proceedings on confiscation of the illegally acquired property; and (iii) assets on which precautionary measures have been imposed.

- (d) *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. Relevant data is collected in the Register of NRA as per *Order on the Register of NRA*.

Weighting and Conclusion

3. All criteria are met. **R.33 is re-rated compliant.**

Annex B: Summary of Technical Compliance – Deficiencies underlying the ratings

Recommendations	Rating	Factor(s) underlying the rating ⁷
2. National co-operation and co-ordination	PC (MER) LC (FUR1 2024)	<ul style="list-style-type: none"> Despite the fact that the SANS is appointed to carry out the counter proliferation co-ordination between the competent authorities, there are no specific co-operation and co-ordination mechanisms to combat PF on the operational level (c.2.4 - MER).
12. Politically exposed persons	PC (MER) LC (FUR1 2024)	<ul style="list-style-type: none"> There is no explicit requirement to conduct enhanced scrutiny on the “whole” business relationship with the policy holder before the pay-out (c.12.4 - MER).
13. Correspondent banking	PC (MER) PC (FUR1 2024)	<ul style="list-style-type: none"> Requirements to: (i) determine from publicly available information the reputation of the institution and the quality of the supervision; (ii) assess the respondent institution’s AML/CFT controls; and (iii) define and document the respective AML/CFT responsibilities of each institution apply to respondent institutions from EU/EEA Member States only when a higher risk is identified (c.13.1 – MER).
14. Money or value transfer services	PC (MER) C (FUR1 2024)	
15. New technologies	PC (MER) PC (FUR1 2024)	<ul style="list-style-type: none"> Lack of holistic risk assessment by the country when analysing new technologies-related risks which does not explicitly cover the use of developing technology (c.15.1 - MER). Apart from the general requirement to mitigate risks, there is no explicit reference to taking appropriate measures to manage and mitigate risks that specifically target new products and new business practices, new delivery mechanisms or new and developing technologies (c.15.2(b) - MER).

7. Deficiencies listed are those identified in the MER unless marked as having been identified in a subsequent FUR.

- There are no legal provisions that would prevent criminals' associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP (c.15.4(b) – MER).
- No proactive action is taken by the authorities to identify natural or legal persons carrying on VASP activities without a prior registration (c.15.5 MER).
- There are no legal provisions enabling restriction or suspension of a VASP's registration (15.6(b)- MER).
- No VASP-specific AML/CFT guideline is issued (c. 15.7 - MER).

The following deficiencies under R.34 are also applicable (c.15.7 – MER):

- 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 the broad range of products and services that fall under AML/CFT legislation (c.34.1 – MER).
- Very limited consolidated feedback is being provided by FID-SANS to OEs to assist them in detecting and reporting suspicious transactions (c.34.1 – MER).
- Guidance on specific red flags has been provided only to banks; other sectors have not been covered (c.34.1 – MER).

The following deficiency under R.35 is also applicable (c.15.8 - MER):

- Monetary penalties, including those applicable to directors and senior management are not always fully dissuasive (c.35.1-35.2 – MER).

The following deficiencies under R.10, R.13, R.16 and R.20 are also applicable (c.15.9 - MER):

- Bulgarian legislation allows for an alternative method to identify and verify legal persons and arrangements, i.e., it is permitted not to request

		<p>certified identity documents from legal persons provided that legal personality information can be obtained from EU registers (c.10.9 – MER).</p> <ul style="list-style-type: none"> • There is no explicit requirement to identify and take reasonable measures to verify the identity of a natural person who exercises control through other means than ownership in some circumstances (c.10.10 – MER). • There is no explicit requirement to take into account materiality and varying risk levels (except for higher-risk customers and relationships) (c.10.16 – MER). • There is no explicit requirement to conduct due diligence at appropriate times, taking into account whether and when CDD measures have been previously undertaken and the adequacy of data obtained (c.10.16 – MER). • Requirements to: (i) determine from publicly available information the reputation of the institution and the quality of the supervision; (ii) assess the respondent institution’s AML/CFT controls; and (iii) define and document the respective AML/CFT responsibilities of each institution apply to respondent institutions from EU/EEA Member States only when a higher risk is identified (c.13.1 – FUR 1). • 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 (c.16.17 – MER). • There is no explicit requirement to report in cases where there are reasonable grounds to suspect ML/TF (c.20.1 – MER). • EU Regulation (EU) 2015/847 which provides the legal basis for compliance under the R.16 is not applicable to
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>VASPs. (c.15.9(b) - MER)</p> <p>The following shortcomings under R.7 are also applicable (c.15.10 - MER):</p> <ul style="list-style-type: none"> • It is not clear which is the competent authority to report to on assets frozen or actions taken. Attempted transactions are not precisely covered (c.7.2(e) – MER). • At national level, Bulgaria did not adopt measures for monitoring and ensuring compliance by with relevant laws or enforceable means governing the obligations under R.7. Failure to comply with such laws or enforceable means is not subject to civil, administrative or criminal sanctions (c.7.3 – MER). • Bulgaria does not have mechanisms for communicating de-listings and unfreezing immediately upon taking such action, and providing guidance to persons that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action (c.7.4(d) – MER). <p>The following shortcomings under R.37 to R.40 are also applicable (c.15.11):</p> <ul style="list-style-type: none"> • Deficiencies identified in R.3 and R.5 apply (c.37.7 and c.39.1(a) – MER). • For non-EU countries there are no rules to provide for any expeditious action in the field of detection, seizure and confiscation. Dual criminality is not required by the CPC but, indirectly, by other international instruments in this field (c.38.1 – MER). • Provisional measures pursuant to Art. 72 CPC cannot be applied if the perpetrator is unknown or is dead (c.38.2 – MER). • Mechanisms available for 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 (c. 38.3 (b) – MER).
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

18. Internal controls and foreign branches and subsidiaries	PC (MER) LC (FUR1 2024)	<ul style="list-style-type: none"> • There is no explicit obligation to provide assistance rapidly or in a timely manner, except for FIU-to-FIU co-operation under the LMML (c. 40.1 – MER). • In regard to LEAs (SANS) there are no explicit legal provisions providing for timely exchange of information (c.40.2(d) – MER). • There is no legal basis for supervisors to conclude agreements with non-EU Member States (c.40.12 and c.40.14 – MER). • It is not clear if IOCD can exchange information with other competent authorities that are not their counterpart (c.40.20 – MER). • There is no requirement for an independent audit function to test systems (c.18.1(d) - MER).
22. DNFBPs: Customer due diligence	PC (MER) LC (FUR1 2024)	<p>The following shortcomings under R.10 and R.15 are also applicable (c.22.1 and c.22.4 - MER):</p> <ul style="list-style-type: none"> • See R.15 (c.10.9, c.10.10 and c.10.16 - MER) above. • See R.15 (c.15.1 and c.15.2(b) - MER).
25. Transparency and beneficial ownership of legal arrangements	PC (MER) LC (FUR1 2024)	<ul style="list-style-type: none"> • 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. (c.25.1(c) - MER) <p>Shortcomings under R.35 are applicable (c.25.7 - MER):</p> <ul style="list-style-type: none"> • Monetary penalties, including those applicable to directors and senior management are not always fully dissuasive (c.35.1-35.2 – MER).
26. Regulation and supervision of financial institutions	PC (MER) LC (FUR1 2024)	<ul style="list-style-type: none"> • Entry controls for some FIs do not explicitly prevent licensing/registration in case of association with criminals, in particular: (a) associates of criminals are not covered for PMOs; and (b) entry controls do not extend to BOs of

<p>27. Powers of supervisors</p> <p>32. Cash Couriers</p> <p>33. Statistics</p>	<p>PC (MER) LC (FUR1 2024)</p> <p>PC (MER) C (FUR 2024)</p> <p>PC (MER) C (FUR 2024)</p>	<p>currency exchange offices or managers of insurance operators and intermediaries (c.26.3 - MER).</p> <ul style="list-style-type: none"> • There is no explicit requirement to determine the frequency and intensity of supervision based on characteristics of FIs and financial groups, including diversity and number (c.26.5(c)) - MER). • 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 (c.26.6) - MER). • Deficiencies exist in the range of sanctions are that are available to supervisors (c.27.4 - MER).
---------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering and combating financing of terrorism
AT	Assessment team
BGN	Bulgarian Leva
BNB	Bulgarian National Bank
BNIs	Bearer-negotiable instruments
BO	Beneficial Owner
BORIS	BO Registers in other Member States via the European e-Justice Portal
BRA	Business risk assessment
C	Compliant
CDD	Customer Due Diligence
CIS	Customs Information System
CISOUCIA	Collective Investment Schemes and Other Undertakings for Collective Investments Act
CRC	Communications Regulation Commission
CACIAF	Commission for Anti-Corruption and Illegal Assets Forfeiture
DNFBPs	Designated non-financial businesses and professions
ECB	European Central Bank
EEA	European Economic Area
EMI	Electronic money institution
EU	European Union
FATF	Financial Action Task Force
FID-SANS	Financial Intelligence Directorate of State Agency for National Security
FI	Financial Institution
FIU	Financial Intelligence Unit
FSC	Financial Supervision Commission
FSCA	Law on the Financial Supervision Commission
FUR	Follow-up report
IAIS	International Association of Insurance Supervisors
IC	Insurance Code
IMF	International Monetary Fund
IO	Immediate Outcome
IT	Information Technology
LC	Largely compliant
LCI	Law on Credit Institutions
LEA	Law Enforcement Agency
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
MER	Mutual evaluation report
MFIA	Markets in Financial Instruments Act
MLA	Mutual Legal Assistance
ML/TF	Money laundering/terrorist financing
MoI	Ministry of Interior

MVTS	Money or value transfer services
NaRA	National Revenue Agency
NC	Non-compliant
NCA	National Customs Agency
NRA	National Risk Assessment
NRAM WG	
OE	Obligated entity
PC	Partially compliant
PEP	Politically exposed person
PMOs	Postal money order (operators)
PoC	Point of contact
PI	Payment Institution
PMO	Postal money order (operators)
R.	Recommendation
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
SIC	Social Insurance Code
STR	Suspicious transaction report
TC	Technical compliance
TFS	Targeted financial sanctions
UNSC	United Nations Security Council
VA	Virtual asset
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 2024

Anti-money laundering and counter-terrorist financing measures -

Bulgaria

1st Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Bulgaria's progress in addressing the technical compliance deficiencies identified in the May 2022 assessment of their measures to combat money laundering and terrorist financing.

Follow-up report