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(2023)20

Anti-money laundering and counter-terrorist financing measures

Serbia

5th Enhanced Follow-up Report & Technical Compliance Re-Rating

December 2023

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 5th Enhanced Follow-up Report and Technical Compliance Re-Rating on Serbia was adopted by the MONEYVAL Committee through written procedure (7 December 2023).

Serbia: 5th Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER) of Serbia[1] was adopted in April 2016. Given the results of the MER, Serbia was placed in enhanced follow-up.[2] Its first follow-up report (FUR) was submitted in September 2017; however, it was tabled for information only. Its second,[3] third[4] and fourth[5] enhanced follow-up reports were adopted in December 2018, December 2019 and November 2021 respectively. The report analyses the progress of Serbia in addressing the technical compliance (TC) deficiencies identified in its fourth enhanced FUR. 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. This report does not address what progress Serbia has made to improve its effectiveness.

2. The assessment of Serbia's request for technical compliance re-rating and the preparation of this report were undertaken by Malta's Rapporteur team (together with the MONEYVAL Secretariat).

3. Section II of this report summarises Serbia's progress made in improving technical compliance. Section III sets out the conclusions 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 Serbia to improve its technical compliance by addressing the technical compliance deficiencies identified in the 4th Enhanced FUR for which the authorities have requested a re-rating (R. 15).

5. Serbia is not rated partially complaint (PC) in relation to other Recommendations.

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 Serbia submitted its country reporting template – at least six months before the FUR is due to be considered by MONEYVAL.[6]

II.1 Progress to address technical compliance deficiencies identified in the MER and applicable subsequent FURs

7. Serbia has made sufficient progress to address the technical compliance deficiencies identified in the 4th enhanced FUR. As a result of this, Recommendation 15 has been upgraded to largely compliant (LC).

8. Annex A provides the description of country's compliance with Recommendation 15 that is reassessed, set out by criterion, with all criteria covered. Annex B provides the consolidated list of remaining deficiencies of the re-assessed Recommendation.

1. Mutual evaluation report available at https://rm.coe.int/anti-money-laundering-and-counter-terrorist-financing-measures-serbia-/1680715fdb.
2. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
3. Report available at https://rm.coe.int/committee-of-experts-on-the-evaluation-of-anti-money-laundering-measur/1680931ea5.
4. Report available at https://rm.coe.int/anti-money-laundering-and-counter-terrorist-financing-measures-serbia-/1680998aa8.
5. Report available at https://rm.coe.int/moneyval-2021-34-fur-serbia/1680a4db3a.
6. 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 Serbia since its MER or the 2nd, 3rd, 4th and 5th enhanced FURs were 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, December 2023[7]

R.1	R.2	R.3	R.4	R.5
LC (FUR 2018) ~~PC~~	LC (FUR 2019) LC	LC	LC	LC
R.6	R.7	R.8	R.9	R.10
LC (FUR 2019) ~~PC~~	LC (FUR 2018) ~~NC~~	LC (FUR 2019) ~~PC (FUR 2018)~~ ~~PC~~	LC	LC (FUR 2018) ~~PC~~
R.11	R.12	R.13	R.14	R.15
LC	C (FUR 2018) ~~PC~~	LC (FUR 2018) ~~PC~~	LC	**LC (FUR5 2023)** ~~PC (FUR 2021)~~ ~~LC~~
R.16	R.17	R.18	R.19	R.20
LC (FUR 2018) ~~PC~~	C	C (FUR 2019) ~~PC~~	LC (FUR 2018) ~~PC~~	C
R.21	R.22	R.23	R.24	R.25
C	LC (FUR 2021) ~~PC (FUR 2018)~~ ~~PC~~	LC (FUR 2021) ~~PC (FUR 2018)~~ ~~PC~~	LC	LC (FUR 2018) ~~PC~~
R.26	R.27	R.28	R.29	R.30
LC (FUR 2019) ~~PC~~	LC	LC (FUR 2021) ~~PC~~	LC	LC
R.31	R.32	R.33	R.34	R.35
LC	LC	LC	LC	LC (FUR 2018) ~~PC~~
R.36	R.37	R.38	R.39	R.40
LC	LC	LC	LC	LC (FUR 2021) ~~PC (FUR 2018)~~ ~~PC~~

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

10. Serbia has implemented all 40 Recommendations at the level of LC/C; therefore, no further reporting shall be required under MONEYVAL's 5th round of evaluations.

7. Recommendations with an asterisk are those where the country has been assessed against the new requirements following the adoption of its MER or FUR.

Annex A: Reassessed Recommendations

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	[2016]	[LC]
FUR2	[2018]	[LC] (no upgrade requested)
FUR3	[2019]	[LC] (no upgrade requested)
FUR4	[2021]	[↓PC] (new requirements)
FUR5	[2023]	[↑LC] (upgrade requested)

1. Serbia was rated LC with the previous Recommendation 8. The MER noted that the requirements to consider new technologies do not apply to all financial institutions (FIs) and that, having recently been introduced; further guidance and monitoring were needed before the requirements could be assessed as fully implemented. All the shortcomings stated in the MER were rectified by the time of the 4th FUR, however as Recommendation 15 was modified to address challenges relating to virtual asset service provider (VASPs) and virtual asset (VA) activities, Serbia's level of compliance was downgraded from LC to PC.

2. **Criterion 15.1** – Article 37 of the AML/CFT Law obliges all reporting entities to assess risks that may arise in relation to new technologies. In addition, similar requirements for FIs are foreseen in Section 9 of the Decision on Guidelines for the Application of the AML/CFT Law.

3. **Criterion 15.2** – Article 37 of the AML/CFT Law obliges reporting entities to assess and mitigate money laundering/terrorist financing risks prior to the launch of a new technology, product or service.

4. **Criterion 15.3** –

(a) Serbia has conducted an ML/FT Risk Assessment in the VA Sector in 2021 as a result of which this sector was considered as posing a medium level of risk. The national risk assessment (NRA) was led by a working group composed of relevant representatives from several authorities. Additionally, data received from the private sector, including VASPs, FIs and designated non-financial businesses and professions was also analysed. The NRA refers to a number of relevant mitigating measures, such as extensive supervision being carried out, a restrictive regime on the use of VAs by financial institutions, strict regulatory requirements on financial institutions and VASPs. Additionally, the National Bank of Serbia (NBS) website lists licensed VASPs, which enables monitoring of unlicensed activity. A Register of Virtual Currency Holders was also established. The NRA also makes reference to a number of threats including cryptocurrency theft, fraud, ransomware, Ponzi schemes and drug and arms trafficking through the dark net. For the analysis of the national risks in the VA sector, Serbia utilised a range of quantitative data, including: (i) replies from questionnaires by the private sector; (ii) data on types of VA services offered by VASPs; (iii) data on VASPs' clients and on VAs used by VASP clients; (iv) data on the entry of VAs into the financial system; (v) data on transactions with cryptocurrencies that are the product of illicit activities; and (vi) data on the temporary and permanent seizure of VAs.

While authorities place great emphasis on the supervisory measures, this control is yet to be assessed given that in 2021, no licenses had been issued. Although supervision on VASPs' AML/CFT obligations had been ongoing since 2018, no data on the results of such supervision was utilised. The supervisory authorities identified notably nine companies and one natural person which were providing services related to virtual currencies without being authorised to do so. While there is reference to suspicious transaction report, it remains unclear how this information was utilised to better identify the threats identified.

Overall, the Republic of Serbia has carried out a comprehensive assessment of risks in the VA sector, has understood the threats and vulnerabilities in the Sector and has identified and implemented good levels of controls to manage risks. However, there are still some aspects which can be further improved such as in ensuring that the main body of the text is reflected in the matrices and conclusions being reached.

(b) The country's action plan lists valuable actions (e.g. the prioritisation of onsite inspections during the first year of licensing, identifying persons engaging in unauthorised provision of VA services, etc.) and the NBS has already started an inspection over one of the two VASPs licensed in the Republic of Serbia, with the inspection on the second VASP targeted for the last quarter of 2023. However, the control measure on supervisory reviews and the implementation of a risk-based approach is still to be assessed.

(c) According to Article 6 of the AML/CFT Law, VASPs shall develop and regularly update a money laundering and terrorism financing risk analysis (…). The risk analysis from paragraph 1 of this Article shall be commensurate to the nature and scope of business operations and the size of the obliged entity, shall consider basic types of the risk (customer, geographic, transaction and service (which also includes services and delivery channels)) and other types of the risk the obliged entity has identified based on the specific character of its business. VASPs are required to document their risk assessment (paragraph 1 of Article 95 of the AML/CFT Law), consider all relevant factors (Article 6 of the AML/CFT Law, Section 6 of the Guidelines), keep the risk assessment up to date (paragraph 1 of Article 6 of the AML/CFT Law), as well as provide the risk assessment to competent authorities (paragraph 4 of Article 6 of the AML/CFT Law).

According to Article 92 of the Law on Digital Assets a digital asset service provider shall establish, maintain and improve reliable, efficient and comprehensive governance and internal controls systems that ensure responsible and reliable management of such digital asset service provider. According to paragraph 1 of Section 19 of the Guidelines internal acts of obliged entities are required to be approved by top management. VASPs are required to monitor the implementation of internal controls and to enhance them if necessary (Article 92 of the Law on Digital Assets).

5. **Criterion 15.4** – According to item 5 of Article 2 of the Law on Digital Assets provides for a definition of VASPs means a legal person which provides one or more services related to digital assets, which are enumerated in Article 3 of the Law on Digital Assets, and it can be only a company regardless of the legal form of company (e.g. limited liability company, joint stock company, etc). Article 3 of the Law on Digital Assets provides for an exhaustive list of services that can be provided, which is fully in line with the FATF definition of VASPs. According to paragraph 1 of Article 4 of the Law on Digital Assets VASPs are required to obtain a license to provide VA services. In order to provide VA services by foreign VASPs on the territory of Serbia (Article 52 of the Law on Digital Assets), such companies are required to establish a Serbian legal person. Branches or other organisational parts of VASPs registered abroad may not provide VA services in Serbia. If the NBS or Securities Commission find that foreign VASP is physically present and offers services in Republic of Serbia, they shall consider that as an unauthorised provision of services related to VAs and commence an appropriate procedure.

(a) The Law on Digital Assets only empowers companies, i.e. legal persons to provide VA (Article 4, paragraph 1 of the Law on Digital Assets).

(b) Articles 60, 65 and 68 of Law on Digital assets establish the necessary requirements to prevent criminals and their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP.

6. **Criterion 15.5** – Control of meeting all the conditions for obtaining the licence for providing VA services is carried out continuously after obtaining the license and if the supervisory authority

(the National Bank of Serbia or Securities Commission) establishes that a VASP no longer meets that conditions, it may pass a decision revoking the licence for the provision of VA services (Article 137, paragraph 2, item 1 of the Law on Digital Assets). Also, authorities are empowered to impose criminal sanctions (Article 353 of the Criminal Code).

7. Apart from preventative measures and sanctions, the Serbian authorities on permanent basis carry out identification of potential illegal VASPs by collecting data from publicly available sources of information (by searching the Internet and the media), from reports of the competent authorities (e.g. law enforcement authorities), as well as from reports of VASPs that are subject to supervision of the National Bank of Serbia.

8. **Criterion 15.6** –

(a) VASPs that provide services related to VA are supervised by the National Bank of Serbia (point 4 of paragraph 1 of Article 2 of the Law on Digital Assets). VASPs that provide services related to digital tokens are supervised by the Securities Commission (point 4 of paragraph 1 of Article 2 of the Law on Digital Assets).

Both supervisors carry out risk-based supervision of obliged entities in accordance with Article 104 paragraph 4 of the AML/CFT Law. Sub-items of paragraph 4 of Article 104 of the AML/CFT Law provide a list of factors that should be considered by the supervisors. In addition, the NBS Methodology provides supplementary factors to be considered by the NBS, which are in line with requirements of c.26.5. Similar criteria are considered by the Securities Commission when conducting their risk-based supervision. The NBS has also implemented a methodology for carrying out of risk-based supervision. This methodology takes into consideration a number of risk factors for the assessment of the inherent risks as well as a number of considerations for assessing the level of controls in place. Also, VASPs are required to notify the Authority of the introduction of a new product and provide all relevant documentation including a risk analysis of such new product. In determining the inherent risks arising from the products the Methodology consider instances where a product can be abused. However, the Methodology should be enhanced further in understanding how a product or service may be abused such as by assessing the abuse of transfer to un-hosted wallets.

(b) The supervisory authorities are vested with necessary powers to ensure compliance of VASPs with the AML/CFT requirements (Article 109, paragraph 7 and Article 110, paragraph 1 of the AML/CFT Law, Article 124, paragraph 1 and Article 125, paragraph 1 of the Law on Digital Assets).

Supervisory authorities have powers to impose a range of administrative sanctions to VASPs that fail to implement the provisions of that Law and the AML/CFT Law, which range from a recommendation (which should be issued for minor irregularities or deficiencies), through a letter of warning and order to eliminate the established irregularities, to withdrawing the license (which shall be issued for major violation of the provisions of the AML/CFT Law and for failing to allow the supervisory authority to perform supervision) (Article 135 of the Law on Digital Assets).

The supervisory authority may also pass a decision on partial revoking the licence for the provision of VA services, so as to prohibit the provision of certain VA services covered by that licence i.e. to limit the licence to a certain VA services only (Article 135, paragraph 2, item 5 of the Law on Digital Assets).

9. **Criterion 15.7** – According to Article 114 of the AML/CFT Law, the supervisory authorities can issue recommendations and/or guidelines for implementing the provisions of this Law, independently or in co-operation with other authorities. The authorities have already issued the

Decision on Guidelines for the Application of the Provisions of the Law on the Prevention of Money Laundering and Terrorism Financing for Obligors Supervised by the National Bank of Serbia, which also applies to VASPs.

10. The National Bank of Serbia, as supervisory authority, provides VAPSs with information and press releases regularly through its website (NBS | Prevention of money laundering and the financing of terrorism), but also has a direct channel of communication with all obliged entities, so it provides them with answers and opinions regarding its AML/CFT regulations and in co-operation with administration for the prevention of money laundering (APML) provides them also with the answers on questions regarding the AML/CFT Law (such answers and opinions are available on APML website: http://www.apml.gov.rs/pretraga-strucnih-misljenja – in Serbian language only).

11. **Criterion 15.8** –

(a) Serbian authorities are empowered to impose civil and administrative sanctions on VASPs for failure to comply with the AML/CFT Law and the Law on Digital Assets Articles 132 to 137 of the Law on Digital Assets and Article 109, paragraph 7 and Article 110, paragraph 1, Article 117-120 of the AML/CFT Law. Sanctions for violations of the requirements under the UN sanctions regime are stipulated in Articles 18 and 19 of the Law on the Freezing of Assets with the Aim of Preventing Terrorism (LFA). The competent authority to supervise compliance with the LFA is the APML, which can request elimination of irregularities or apply to the prosecutor to initiate misdemeanour proceedings with the view of imposing a pecuniary fine. Sanctions range from a recommendation (which should be issued for minor irregularities or deficiencies), through a letter of warning and order to eliminate the established irregularities, to withdrawing the license. These sanctions can be considered dissuasive and proportionate.

(b) The fines for the member of the managing body and director of the VASP can range up to RSD 1,000,000 (approximately EUR 8,500) (Article 136, paragraph 2 of the Law on Digital Assets). A natural person may be subject to the fine even if, at the time of pronouncing a fine, the person no longer acts in the capacity of a member of the managing body or director of the VASP. Also, the member of the managing body or the director can be dismissed if they act in breach of the Law on Digital Assets. The Criminal Code and the Law on Confiscation of Property Originating from Criminal Offences are also applicable to VASPs and their responsible persons. These sanctions cannot be considered proportionate and dissuasive.

12. **Criterion 15.9** – Deficiencies under R.10, 11, 13,16 and 19 apply to c.15.9.

13. Serbia requires VASPs to obtain information on the legal form of a customer as per Article 99 of the AML/CFT Law, as well as to identify and verify the identity of the legal person, the representative of the customer as well as the empowered representative with whom the obliged entities deal with. However, deficiencies still remain in obtaining information on the powers that regulate and bind the legal person and the names of the person having senior management positions (c.10.9).

14. Article 7, paragraph 4 of the AML/CFT Law requires obliged entities to cease the conduct of customer due diligence (CDD) if such would raise the suspicion of the customer. Obliged entities must make an official note of this and send it to the APML. This Article is also applicable to VASPs. In June 2021, the NBS also enacted amendments to the Guidelines for the Application of the Provisions of the Law on the Prevention of Money Laundering and Terrorism Financing for Obligors Supervised by the National Bank of Serbia to extend the general application of these Guidelines, which include CDD requirements, to VASPs (c.10.20).

15. Article 95 of the AML/CFT Law requires VASPs to keep data and documentation on customers, business relationships, risk assessments and transactions for at least 10 years from the date of termination of the business relationship and/or the execution of a transaction "business relationships". However, the AML/CFT Law does not explicitly oblige reporting entities to keep

account files and business correspondence. Moreover, there is no reference in relation to analyses for deciding on the external dissemination (c.11.2).

16. Reporting entities are still not clearly required to understand the nature of the respondent's business in case of VASPs (c.13.1 (a) (b)). The Travel Rule for VASPs has been implemented by Article 15a to 15c of the AML/CFT Law. It provides for the obtaining and transmission of data related to the name and surname or business name of all persons participating in the VA related transaction including whether the person is the originator or beneficiary of the transactions, the address or address of the registered office of those persons, the VA address used to execute the transaction or the corresponding unique identifier of this transaction. The VASP executing the transaction is obliged to ensure such data is sent at the time of execution and the VASP receiving the transaction shall ensure that such data is received upon execution. However, the AML/CFT Law does not include specific provisions regarding batch files (c.16.1, 16.2).

17. VASPs are required to apply enhanced due diligence measures when exposed to countries with strategic deficiencies. VASPs are also not allowed to establish a branch and/or directly provide virtual currency services in a country which regulations are not harmonised with international AML/CFT standards. In terms of Article 41 authorities can issue a call for specific countermeasures including for example limiting financial transactions and business relationships with customers from such countries or to issue call for other countermeasures as necessary to eliminate risks (c.19.2).

(a) According to paragraph 2 of Article 75 of the Law on Digital Assets VASPs are required to establish business relationship irrespective of any threshold with each user of VAs and establish and verify his identity in accordance with the AML/CFT Law.

(b) (i) Article 15a of the AML/CFT Law requires originating VASPs to obtain all required information on all persons participating in the VA transfer. This information is verified pursuant to Articles 17-23 of the AML/CFT Law. The obtained data shall be provided to another VASP at the same time as the execution of the VA related transaction and in a manner that ensures the integrity of that data and protection against unauthorised access to that data. Originating VASP is obliged to hold this data in accordance with the AML/CFT Law and make it available without delay at the request of the supervisory authority, the Administration for the Prevention of Money Laundering or other competent authority. (Article 15a of the AML/CFT Law).

(ii) Beneficiary VASP is obliged to hold data in accordance with the AML/CFT Law and make it available without delay at the request of the supervisory authority, the Administration for the Prevention of Money Laundering or other competent authority. (Article 15b of the AML/CFT Law).

(iii) VASPs are required to monitor the availability of information (Article 15c of the AML/CFT Law) and to take freezing actions and prohibit transactions with designated persons and entities as foreseen by the Law on the Freezing of Assets with the Aim of Preventing Terrorism and Financing of Proliferation.

(iv) FIs are prohibited from providing VA activities apart from brokers (Article 13 of the Law on Digital Assets). If a broker is involved in sending or receiving virtual asset transfers on behalf of a customer, he is required to comply with requirements of Articles 15a-15c of the AML/CFT Law.

18. **Criterion 15.10** – The communication mechanisms, reporting obligations and monitoring referred to in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) equally apply to VASPs.

19. **Criterion 15.11** – Supervisors of VASPs are empowered to provide international co-operation according to Article 127 of the Law on Digital Assets and Article 112a of the AML/CFT Law. However, deficiencies under R.37-40 have a negative impact.

20. It remains unclear whether authorities have in place processes for the prioritisation and timely execution of requests. It is also unclear whether other authorities (e.g. supervisors, tax authorities), excluding the police and the APML have clear and secure means for the exchange of information (c.40.2).

21. Article 22 of 2019 Convention on Mutual Administrative Assistance in Tax Matters provides safeguards and confidentiality for data exchange between parties to this convention. Where there is no international agreement on the exchange of secret data, the Law on Secret Data applies. Also, the Personal Data Protection Act as a basic condition for the exchange of personal data, requires establishing the clear purpose for the exchange and to ensure mandatory level of data protection. Article 7 of the Law on Tax Procedure and Tax Administration covers the range of data that is considered confidential and also prescribes that the level of confidentiality also applies in case of international co-operation in line with Article 157 (c.40.6-40.7).

22. Article 127, paragraph 4 of the Law on Digital Assets, provides that the supervisory authority shall co-operate with the competent authorities of foreign countries and, may exchange data with them on prudential matters including unauthorised activity. Additionally, Article 112a of the AML/CFT Law provides for the sharing of information between Competent Authorities on AML/CFT matters (c.40.12 – 40.16).

Weighting and Conclusion

23. The AML/CFT Law requires reporting entities to identify and assess the ML/FT risks in relation to the use of new technologies. Meanwhile, reporting entities are obliged to undertake risk assessments prior to introducing new products and to adopt measures to manage and mitigate the identified risks. Serbia is compliant with the requirements to license or register VASPs, identify persons carrying out VASP activities, to regulate the sector, provide guidelines and feedback to VASPs, obligations relating to targeted financial sanctions. Serbia has also carried out a risk assessment of the VASP sector. The implementation of the risk-based approach is still to be assessed. Deficiencies identified under preventive measures and international co-operation equally apply to R. 15. **Therefore, R. 15 is re-rated Largely Compliant**.

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

Recommendations	Rating	Factor(s) underlying the rating[8]
15. New technologies	PC (MER) PC (FUR 2022) LC (FUR5 2023)	• The NRA still lacks an assessment of the quality of supervisory intervention (c.15.3(a)). • Lack of understanding in relation to the risks and potential abuse of products and services offered by VASPs (c.15.6 (a)). • The effectiveness of control measure on supervisory reviews and the implementation of a risk-based approach should be demonstrated (c.15.3(b)). • Notwithstanding the fact of availability of sanctions, they cannot be considered as proportionate and dissuasive (c.15.8 (b)). • c.15.9 The law does not oblige FIs to obtain information on the powers that regulate and bind the legal person and the names of the persons having senior management positions (c.10.9). • c.15.9 No explicit requirement for reporting entities to keep account files, business correspondence and records of analysis carried out (c.11.2). • c.15.9 Reporting entities are still not clearly required to understand the nature of the respondent's business (c.13.1(a)). • c.15.9 The Law does not require an assessment of the AML/CFT measures applied by the respondent (c.13.1(b)). • c.15.9 Serbia has also not introduced specific provisions regarding batch files (c.16.2). • c.15.11 Minor deficiencies mentioned in the MER regarding sub-criteria 40.2(c) and 40.2(d) remain. Clarity about the prioritisation and timely execution of requests as well as clear and secure means of exchanging information.

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

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering/countering the financing of terrorism
APML	Administration for the prevention of money laundering
C	Compliant
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
FATF	Financial Action Task Force
FI	Financial institution
FUR	Follow-up report
LC	Largely compliant
LFA	Law on the reezing of Assets with the Aim of Preventing Terrorism
MER	Mutual evaluation report
ML/TF	Money laundering/terrorist financing
NBS	National Bank of Serbia
NC	Non-compliant
NRA	National risk assessment
PC	Partially complaint
R.	Recommendation
VA	Virtual asset
VASP	Virtual asset service provider
TC	Technical compliance

www.coe.int/MONEYVAL

December 2023

Anti-money laundering and counter-terrorist financing measures -

Serbia

5th Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Serbia's progress in addressing the technical compliance deficiencies identified in the April 2016 assessment of their measures to combat money laundering and terrorist financing and subsequent follow-up reports.

The report also looks at whether Serbia has implemented new measures to meet the requirements of FATF Recommendations that changed since the 2016 assessment.

Follow-up report