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)19

Anti-money laundering and counter-terrorist financing measures

Slovak Republic

3rd Enhanced Follow-up Report & Technical Compliance Re-Rating

December 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 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating on Slovak Republic was adopted by the MONEYVAL Committee at its 68th Plenary Meeting (Strasbourg, 5 December 2024).

Slovak Republic: 3rd Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER)[1] of Slovak Republic was adopted in September 2020. Given the results of the MER, Slovak Republic was placed in enhanced follow-up.[2] Its 1st enhanced follow-up report (FUR) was adopted in November 2022,[3] the 2nd FUR was adopted in December 2023.[4] The report analyses the progress of Slovak Republic in addressing the technical compliance (TC) deficiencies identified in its MER or subsequent FURs. 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 Slovak Republic for three technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur teams (together with the MONEYVAL Secretariat):

- Georgia

3. Section II of this report summarises Slovak Republic's progress in improving technical compliance. Section III sets out the conclusion and a table showing which recommendations (R.) have been re-rated.

II. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

4. This section summarises the progress made by Slovak Republic to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER and applicable subsequent FURs for which the authorities have requested a re-rating (R. 8, 15, and 19).

5. For the rest of the recommendations rated as partially compliant (PC) (R.10, R.12, R.13, R.18, R.23, R.28, R.29, R.32 and R.35) 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 were in force and effect at the time that Slovak Republic submitted its country reporting template – at least six months before the FUR is due to be considered by MONEYVAL.[5]

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

7. Slovak Republic has made some progress to address the technical compliance deficiencies identified in the MER and applicable subsequent FURs. However, following the analysis of R.8, R.15, and R.19, it was concluded that the progress was not sufficient to justify an upgrade and all reviewed recommendations remain PC.

8. Annex A provides the description of 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. MER of Slovak Republic, available at https://rm.coe.int/moneyval-2020-21-5th-round-mer-slovakia/1680a02853.
2. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
3. 1st enhanced FUR, available at https://rm.coe.int/moneyval-2022-16-fur-sk/1680a9211a.
4. 2nd enhanced FUR, available at https://rm.coe.int/moneyval-2023-21-sk-5thround-2ndenhfur/1680ae98c8.
5. 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.

9. A number of changes have been made since adoption of the MER or subsequent FURs that are relevant for considering recommendations that have been reassessed. Slovak Republic has undertaken several targeted risk assessments, i.e. of the non-profit organisations (NPO) sector targeting the R.8 and one of the virtual asset service providers (VASPs) sector addressing the R.15. In relation to R.19, Slovak Republic has amended the AML/CFT Act to obligate the Financial Intelligence Unit (FIU) to regularly update and publish on its website the list of high-risk jurisdictions with strategic deficiencies identified by Financial Action Task Force (FATF).

III. CONCLUSION

10. Overall, in light of the progress made by Slovak Republic since its MER, 1st enhanced FUR and 2nd enhanced FUR were adopted, its technical compliance with the FATF recommendations has been re-rated as follows.

Table 1. Technical compliance with re-ratings, December 2024[6]

R.1	R.2	R.3	R.4	R.5
LC (FUR1 2022) ~~PC (MER)~~	C (MER)	LC (MER)	LC (MER)	LC (MER)
R.6	R.7	R.8	R.9	R.10
LC (MER)	LC (MER)	PC (FUR3 2024) PC (FUR2 2023) PC (MER)	LC (MER)	PC (FUR1 2022) PC (MER)
R.11	R.12	R.13	R.14	R.15
LC (MER)	PC (FUR1 2022) PC (MER)	PC (FUR1 2022) PC (MER)	LC (MER)	PC (FUR3 2024) PC (FUR1 2022) ~~LC (MER)~~
R.16	R.17	R.18	R.19	R.20
LC (MER)	LC (MER)	PC (FUR1 2022) PC (MER)	PC (FUR3 2024) PC (FUR1 2022) PC (MER)	C (FUR1 2022) ~~PC (MER)~~
R.21	R.22	R.23	R.24	R.25
LC (MER)	LC (MER)	PC (FUR1 2022) PC (MER)	LC (MER)	LC (MER)
R.26	R.27	R.28	R.29	R.30
LC (FUR2 2023) ~~PC (MER)~~	LC (MER)	PC (FUR2 2023) PC (FUR 1 2022) PC (MER)	PC (FUR1 2022) PC (MER)	C (FUR1 2022) ~~PC (MER)~~
R.31	R.32	R.33	R.34	R.35
LC (MER)	PC (FUR 1 2022) PC (MER)	C (FUR 1 2022) ~~PC (MER)~~	LC (MER)	PC (MER)
R.36	R.37	R.38	R.39	R.40
LC (MER)	C (MER)	LC (MER)	LC (MER)	LC (MER)

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

11. The following "big six" recommendation[7] remains PC: R.10. Accordingly, in line with Rule 23 of the Rules of Procedure for the 5th round of mutual evaluations, plenary agreed to place Slovak Republic into compliance enhancing procedures and apply step 1.

6. Recommendations with an asterisk are those where the country has been assessed against the new requirements following the adoption of its MER or FUR.
7. The "big six" recommendations are: R.3, R.5, R.6, R.10, R.11 and R.20.

12. Slovak Republic has not reached the threshold[8] of addressing most, if not all, deficiencies, and so the Plenary may decide in line with Rule 25 of the Rules of Procedure for the 5th round of mutual evaluations to apply compliance enhancing procedures to the following non-"big six" recommendations that remain PC: R.8, R.12, R.13, R.15, R.18, R.19, R.23, R.28, R.29, R.32 and R.35.

13. In line with the Rules of Procedure,[9] the Chair will send a letter to the head of delegation for Slovak Republic drawing their attention to non-compliance with the reference documents and requiring the country to provide a report on recommendation(s) placed under compliance enhancing procedures before the next MONEYVAL Plenary meeting.

14. Slovak Republic will remain under the enhanced follow-up process and is expected to report back to the plenary in one year's time on the progress made in relation to recommendations remaining rated as PC.

8. In line with Rule 30 paragraph 8 of the Rules of Procedure for the 5th round of mutual evaluations, the "threshold" is 36 recommendations at LC/C level. This minimum number may be increased where appropriate to the context of the country.

9 Rule 25, paragraph 4.

Annex A: Reassessed Recommendations

Recommendation 8 - Non-profit organisations

	Year	Rating
MER	2020	PC
FUR1	2022	PC (no upgrade requested)
FUR2	2023	PC (upgrade requested)
FUR 3	2024	PC (upgrade requested, maintained at PC)

1. In the 5th round of evaluations Slovak Republic was rated partially compliant with R.8. The NPO sector was assessed as part of the national risk assessment (NRA) but the subset of NPOs that fall within FATF definition was not identified. No formal review of the adequacy of measures was undertaken, no systematic and specific outreach was conducted, and no best practices were developed. There was no supervision over NPOs, and no specific training was provided to relevant authorities.

2. Slovak Republic's compliance with R.8 was reassessed under its 2nd enhanced FUR in December 2023. Slovak Republic retained a rating of PC, and the following deficiencies remained: no identification of sub-categories that are at risk of terrorism financing (TF) abuse; no review of the adequacy of measures related to the subset of NPO sector that may be abused for TF, and no risk - based approach in supervision of NPOs applied.

3. Since the MER 2020, Slovak Republic has conducted the 2nd NRA (2016-2019) and the targeted sectorial risk assessment of the NPO sector covering period between 2020-2023, published in April 2024 with the aim to review the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for TF support.

4. **Criterion 8.1** –

(a) Article 9 (e) of the AML/CFT Act, defines "a corporation" as a customer being a foundation (as regulated by Act 34/2001 Coll), a non-profit organisation providing services of general economic interest (as regulated by Act 213/1997 Coll.), a non-investment fund (as regulated by Act 147/1997 Coll.) and other special-purpose corporations, irrespective of their legal personality, that manage and distribute funds. The 2nd NRA provides general information on the overall level of risk of TF abuse that NPOs face in Slovak Republic, and gives some examples of activities or characteristics, which are likely to carry a higher risk of TF abuse. The NRA identified the subset of NPOs which would fall within the FATF definition, without detailing the sub-categories which are at risk of TF abuse. According to the sectorial risk assessment (SRA) published in April 2024, civic associations and organisations with an international dimension are legal forms of NPOs that are not required to keep records of their activities or to publish annual reports. This lack of oversight limits the ability to assess NPO activities and identify those at higher risk of TF abuse. While the SRA analysed some characteristics of NPOs, current legislation and regulatory measures, accountability and supervision, interrelations with higher risk countries, it concluded that overall risk level of NPOs TF abuse is low. However, the SRA's limited functional analysis of NPOs prevents a clear determination of which NPOs are at risk when engaging in what specific types of activities and how these characteristics are uniquely applicable to the Slovak Republic's NPO environment.

(b) According to the 2nd NRA, in the period under review (2016-2019), there were no cases where NPOs were used or misused for money laundering (ML) or TF. Similarly, the SRA for 2020-2023 recorded no presence or activities of terrorist organisations in the country, nor any investigations of TF cases involving NPOs. However, the absence of such involvement does not equate to the identification of the nature of threats posed by terrorist entities to the NPOs. Whilst the SRA outlines potential threats, such as returnees from conflict regions

and radicalisation, these scenarios are general in nature and do not link NPO characteristics to the described scenarios. Nonetheless, it must be noted that ways of potential misuse of NPOs for the financing of terrorism are described in the Information for NGOs in the field of combating the financing of terrorism listed on the FIU's website.

(c) Slovak Republic conducted a formal review of the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for terrorism financing support. There were certain shortcomings identified in the oversight and accountability of civil associations and NPOs providing services of general interest, and the necessary recommendations were made accordingly. Furthermore, as concerns remain under 8.1(a) criteria, it is not clear if adequacy of measures has been identified to the full extent. The Register of non-governmental non-profit organisations became operational from 1st of January 2021 and represents a reliable, up-to-date and unified source register of non-governmental NPOs, including data on the beneficial users of NPOs. However, there is no obvious link between the risks identified and the establishment of the registry. Moreover, its establishment was foreseen before the completion of the NRA.

(d) A general provision was introduced as an amendment to the AML Act according to which the NRA shall be submitted to the government for approval, at the latest four years after the previous approval.

5. **Criterion 8.2** –

(a) The Slovak Republic has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs, in particular through specific laws regulating the various legal forms of NPOs, where all relevant data on bookkeeping (single-entry or double-entry accounting) are presented in annual reports, in the register of financial statements, in tax returns, in the register of BOs, while meeting the conditions for applying for a share tax. In the area of transparency of NPOs and their publicly available information, legislative changes were performed in the Slovak Republic. The efficiency of the use of public funds is closely related to the record of non-governmental non-profit organisations. The largest organisations in the NPOs sector in terms of financial volume are foundations, which are also the most controlled and regulated by legislation (Act no. 34/2002 Coll. on Foundations and on Amendments to the Civil Code). Obligations of foundations related to funding control include: the obligation to prepare financial statements and the annual report, the obligation to have the financial statements and the annual report audited by an auditor, the obligation to publish the annual report and deposit it in the register of financial statements, obligation to file a tax return if it has revenue subject to tax (Article. 34 and 35 of the Act no. 34/2002 Coll.).

(b) Specific outreach to the NPO sector or the donor community on FT issues has been conducted. The authorities asserted that the NPOs are notified by the FSJ of possible misuse of terrorist financing in the context of AML/CFT controls that the FIU performs in this sector with four such inspections reported in the period under review. In February 2023, the FIU issued the "Information for NGOs in the field of combating the financing of terrorism" to raise and deepen NPOs awareness on potential vulnerabilities of TF abuse and terrorist financing risks, and updated it in May 2024 as result of a conducted SRA.

(c) As mentioned above, the FIU's document "Information for NGOs in the field of combating the financing of terrorism" contains best practices to address TF risk and vulnerabilities. It also provides a set of steps to be undertaken by the NPO sector to reduce the risks of being misused for TF. The FIU, with involvement of and in cooperation with NPO sector, updated this document to reflect the conclusions of the NPO sectorial risk assessment (April 2024) and following consultation with NPO representatives published on its website an information leaflet "Awareness-raising for NPOs in the area of countering TF".

(d) Foundations are obliged to deposit funds that are part of the foundation assets, to an account at a bank or a branch of a foreign bank. Apart from that, "Information for NGO´s in the field of combating the financing of terrorism" is encouraging NPOs to conduct transactions via regulated financial channels, by providing the risk factors increasing the possibility of NGO abuse, inclusively on the increased use of cash transactions. Additionally, information is available on the National Bank of Slovak Republic's website with the recommendation not to enter into business relationships with "problematic" entities and check the authorisation of individual financial market entities on the National Bank of Slovak Republic's website.

6. **Criterion 8.3** – Slovak Republic does not apply a risk-based approach in supervision of NPOs at risk of TF abuse, but authorities report a number of measures applied to all main types of NPOs according to the AML/CFT Act or according to sectorial regulation (i.e. Act 34/2002 on Foundations, Act 213/1997 on Non-Profit Organisations Providing Public Benefit Services and Act 147/1997 on non-investment funds).

7. For the purposes of the AML/CFT Act, a foundation, a non-profit organisation providing services of general interest, and a non-investment fund are obliged to carry out the identification of the donor and the identification of the natural person or legal entity whose property association has provided funds under Article 25 of the AML/CFT Act, if the value of the donation or the amount of provided funds reach at least 1 000 euros (EUR).

8. The annual reports of a foundation, a non-profit organisation providing services of general interest and a non-investment fund shall be filed in the Register of Financial Statements. All of those shall keep accounts and shall keep accounting records (including annual reports) for the ten years following the year to which they relate (Article 35(3) of Act 431/2002 on Accounting). On the basis of that document retention, the competent authorities may, if necessary, subsequently verify transactions in order to establish whether the funds have been received and spent in a manner consistent with the purpose and objectives of foundations, non-profit organisations and non-investment funds.

9. The authorities report that in the context of their rights and obligations, the Ministry of Interior (MoI) may impose fines on foundations for failure to submit an annual report.

10. The FIU's Methodological Guidance on the selection of the control of obliged entities, amended in April 2024, establishes risk-oriented supervision of obliged entities and pool of assets, including some types of NPOs, based on the ML/TF risk assessment. According to authorities, when considering individual ML/TF factors, FIU would refer to SRA for strategic analysis and consider its findings to supervise covered NPOs. However, the guidance serves as a general tool for the FIU only, and no information was provided regarding supervisory risk-based measures implemented by other competent authorities overseeing NPOs.

11. **Criterion 8.4** –

(a) The authorities stated that the NPO sector is monitored according to the annual controls plan used by the FIU when carrying out controls on entities that show the signs of risk. The FIU has implemented a risk-oriented approach to carrying out controls, as referred to in Article 2.1 of the Order of FIU Director No. 126/2018 and in the Methodological Guidelines on the Procedure for Controlling the Compliance of Obligations of Obliged Persons Pursuant to the AML Act by Police Officers of the Obligation of Controlled Persons of FIU No. 34/2018. After the establishment of the register of non-governmental non-profit organisations, responsible authorities (MoI and district offices), before and after registering a legal person, perform controls on the entities in compliance with the applicable generally binding legal regulation, inclusively by evaluating the Annual Reports. However, as stated under criterion 8.3, Slovak Republic does not apply a risk-based approach to supervision.

(b) The FIU is entitled to conduct controls on NPOs for the purpose of the identification of the beneficial owner (BO) and verification of the veracity and correctness of data about the BO,

for the purpose of identifying persons (donors and recipients of donations worth more than EUR 1 000) or for the purpose of checking disposal of property (Article 25 of the AML/CFT Act). For the non-performance of these obligations, the FIU may impose fines of up to EUR 200 000. (Article 33 (3) AML/CFT Act). If a foundation fails to perform the obligation to deposit an annual report in the public part of the register of financial statements, the Ministry of the Interior may impose a fine of up to EUR 1 000 (paragraph 36 of Act 34/2002 Coll. on Foundations). NPOs are legal entities and are subject to Act No. 91/2016 Coll. on Criminal Liability of Legal Entities. As legal entities, NPOs may be criminally prosecuted for committing the offense of ML under paragraph 233 and paragraph 234 of the Criminal Code, and for the offense of terrorist financing under paragraph 419c of the Criminal Code. Therefore, there is legal basis for the application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.

12. **Criterion 8.5** –

(a) Slovak Republic is effective in NPO related cooperation, coordination and information sharing. If necessary, FIU and law enforcement agency (LEA) are entitled to request information on NPOs from the Register of non-governmental non-profit organisations (including paper documents such as memorandum of association, statutes, annual reports, etc.). NPOs keep accounts according to Act no. 563/1991 on accounting and are subject to control by the tax authorities. Upon request, the tax authorities provide information to the FIU/LEAs. According to paragraph 25 paragraph 2 of the AML Act, the FIU is authorised to carry out inspections on NPOs also for the purpose of property management. In case of unauthorised disposal of assets in NPOs, the FIU withdraws the LEA information. The FIU shall disseminate the information from the unusual transaction reports (UTRs) regarding NPOs to the competent authorities, for example Financial Administration, LEA etc.

(b) The National Counter-Terrorism Unit of the National Criminal Agency is a Police Force unit which has its own investigators and operational search activity specialists who are authorised to examine, detect and investigate suspected terrorist financing. The Slovak authorities provided a detailed list of training activities related to TF issues, inclusively with the implication of NPOs, oriented for the National Counter-Terrorism Unit in order to gain sufficient investigative expertise and capability to examine NPOs suspected of TF abuse/ TF support.

(c) Information on the sub-group of organisations that meet the FATF definition of NPOs (mainly non-profit organisations providing services of general interest and foundations) is provided in the Register of non-governmental non-profit organisations maintained by the MoI of the Slovak Republic. Hence, this information can be obtained in the course of an investigation.

(d) The Slovak Information Service (SIS), FIU and Counter-Terrorism Unit - National Criminal Agency Slovak Republic (CTU – NAKA) can receive and analyse information on any form of TF abuse of NPOs. In addition, on January 1, 2013, the National Security Analytical Center (NBAC) was established within the SIS organisational structure, with the aim of making cooperation among security forces more effective. The key tasks of NBAC are the preparation of comprehensive analytical assessments of security incidents based on reports and statements received from state authorities, monitoring security situation in open sources and the provision of analytical products on security threats to designated recipients. Although no statistics or examples of NPO abuse information sharing were presented to the AT, from the general scope of NBAC one can deduce that such would fall under the attributions of NBAC.

13. **Criterion 8.6** – The FIU uses the procedures and mechanisms for international cooperation that are provided under the AML/CFT Act, to handle information requests regarding NPOs. Joint investigation teams and the Joint Customs Operations are mechanisms which can be used by the

National Counter-Terrorism Unit in the area of the fight against TF under the applicable legislation, including in case a NPO would be involved. Joint investigation teams and Joint Customs Operations have not been used in practice, given that no direct activity by terrorist groups has been recorded so far, and no persons or groups have been localised that would prepare to commit a terrorist offense.

Weighting and Conclusion

14. The NPOs sector was assessed as part of the 2nd NRA and recently in 2024 as a part of a sectorial risk assessment. To some extent, the authorities identified the features and types of NPOs, which are likely to be at risk of terrorist financing abuse, although without detailing which NPOs are at a higher risk of TF abuse based on their specific activities and characteristics. A review of the adequacy of measures, including the subset of NPO sector that may be abused for terrorism financing support has been conducted to a limited extent. Specific outreach to the NPO sector or the donor community on FT issues has been conducted and best practices have been developed in cooperation with NPOs to protect them from TF abuse. It seems that there is a legal base for the application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs. NPO information exchange is carried out in the usual manner by the FIU. Overall, Slovak Republic has addressed some of the deficiencies c.8.1(c) and c.8.2(c), however it still has not identified the NPOs that are at higher risk of TF abuse and does not apply risk-based approach in supervision of NPOs at risk. **Therefore, Slovak Republic remains rated PC with R.8**.

Recommendation 15 – New technologies

	Year	Rating
MER	2020	LC
FUR1	2022	PC (upgrade requested)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (upgrade requested, maintained at PC)

1. In the 5th round MER, Slovak Republic was rated LC with the R.15, as there was no requirement for FIs to conduct risk assessment prior to the launch or use of new business practices and the new or developing technologies.

2. Given the significant revision to R.15, Slovak Republic was reassessed against the requirements in relation to VASPs, as a result of which the rating was downgraded to PC in the 1st FUR adopted in November 2022. The following deficiencies were identified: (i) no explicit requirement for risk management and mitigations in relation to VASPs; (ii) risk-based approach applicable only to entities which have VA/VASPs client in their portfolios; (iii) not all activities provided under FATF definition of VASPs are covered; (iv) the legislation is not clear on the licensing and registration requirements concerning VASPs; (v) no information was provided on the communication mechanisms, reporting obligations and monitoring with respect to targeted financial sanctions (TFS); (vi) lack of market entry requirements in relation to VASPs; (vii) no systemic measures to identify natural or legal persons that carry out VASP activities without the required registration; (viii) no risk-based supervision of VASPs carried out by the FIU; (ix) deficiencies in the VASP risk assessment negatively impact the risk-based supervision; (x) absence of the information regarding the legal processes for withdrawing, restricting or suspending the license for AML/CFT violations; (x) sanctions applicable to VASPs for violations of TFS obligations are not proportionate and dissuasive; (xi) no measures to impose to the directors and senior management of VASPs; no information was provided on how the country ensures travel rule requirements for virtual assets (VA) transfers.

3. In March 2024, the FIU has concluded the VA/VASP sectorial risk assessment and analysed to some extent the risks of VASPs operating in Slovak Republic.

4. **Criterion 15.1** – Article 26a of the AML/CFT Act requires FIU to assess national ML/TF risks and to take into account a number of risk factors provided in Annex No. 2, which include new products, business practices and delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Similarly, Article 20a of the Law requires financial institutions (FIs) to assess their business-specific ML/TF risks taking into account at least the very same risk factors. Article 14(2)(b) further stipulates that FIs must pay special attention to ML/TF risks related to new technologies that favour anonymity.

5. **Criterion 15.2** –

(a) Article 20(1) of the AML/CFT Act requires FIs to update their AML/CFT programs accordingly before starting the provision of new products that increase their ML/TF risk exposure. Hence, FIs are effectively required to assess ML/TF risks before new products are launched. However, no such requirement exists in relation to new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

(b) Article 20a(2) of the AML/CFT Act requires FIs to have in place measures aimed at managing and mitigating risks identified as part of their risk assessments, taking into account the results of NRA, while Article 14(2)(b) specifically requires undertaking proper measures to prevent the misuse of new technologies that favour anonymity. Article 8(1)(a) allows for non-face to face verification of natural persons by FIs. However, the technology used in the process should ensure that the verification is carried out to the same level of reliability as during the physical presence of a customer.

6. **Criterion 15.3** –

(a) The country has taken actions to cover amendments on identifying risks. FIU has concluded VA/VASP sectorial analysis in March 2024 with the involvement of relevant stakeholders. However, only some aspects were covered, and analysis is done to some extent on the risk of VASPs operating in the jurisdiction. The risk assessment is merely based on the questionnaires received from VASPs registered in Slovak Republic, the information received from banks, payment services and electronic money sector considering VASPs as a customer and other information from National Expert Group on Anti-Money Laundering and its members. The country has taken extensive steps in terms of identifying and assessing risks, but it should be noted that the core analysis is based on the limited data, gathered from the registered VASP representatives. The assessment of the relevant part of the VASP sector is constrained due to issues with lack of supervision, statistical data availability and complexity.

(b) Please also refer to c.15.3(a). The actions taken by the country only address application of risk-based approach to entities, which have VA/VASPs clients in their portfolios. Authorities are restrained in applying the risk-based approach, as limitations in regulation, registration/licensing and monitoring processes remain.

(c) Please see analysis under R.1. Covered VASPs are considered obliged persons under the AML/CFT Act (Article 5(o)(p)), and are subject to all provisions of the Act, including the identification and assessment of the ML/TF risks associated with their activities (Article 20a), and implementation of internal control procedures pursuant to Article 20. In relation to c.1.10, covered VASPs are required to provide risk assessment information to the FIU acting as a sole supervisory authority to VASPs (AML/CFT Act, Article 20a(2)). Regarding c.1.11 Slovak Republic has not taken any actions to remedy the identified deficiency.

7. **Criterion 15.4** –

(a) Based on given information, the country has made legislative changes introducing registering requirement for VASPs. However, the Trades Licensing Act does not regulate all activities provided under the FATF definition of VASPs. Activities such as exchange of one VA to another VA, as well as activities on participation in and provision of financial services related to an issuer's offer and/or sale of VA are not covered. Deficiencies under c.15.4(a)(i) and c.15.4(a)(ii) impact this criterion.

(i) Legal and natural persons residing or with the registered office in the territory of the Slovak Republic providing services in the field of virtual currencies are obliged to obtain a trade licence (Trade Licensing Act, Article 5(1) and (4)). As was previously noted, the Trades Licensing Act does not regulate all activities provided under the FATF definition of VASPs.

Authorities explained that registration requirements, as outlined above, would apply to all legal and natural persons residing in or having their registered office in the Slovak Republic, since the law makes no distinction based on whether they operate within the territory of Slovak Republic, outside or both.

(ii) Please refer to analysis under c.15.4(a)(i) as it equally applies to natural persons.

(b) A trade license can be obtained by a natural or a legal person that demonstrates good character, which means absence of criminal record (Trade Licensing Act, Article 6(2)). Authorities indicate that the registering authority verifies this by reviewing the applicant's criminal register. In case of legal entity, the condition of good character must be met by the natural person or persons who are its statutory body, defined as persons authorised to perform legal acts on behalf of the entity. However, it cannot be concluded if there are requirements to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in a VASP. Moreover, the provided legal provisions relate only to criminals and not to their associates.

8. **Criterion 15.5** – Although the authorities provided a case example when they discovered the provision of VASP services without authorisation, no systemic measures are applied to identify natural or legal persons that carry out VASP activities without the requisite license or registration. Unauthorised business activity constitutes a criminal or administrative offence, and is subject to appropriate sanctions upon conviction, including imprisonment of natural person of up to eight years, monetary penalties of unspecified amount, annulment of legal entity, or cessation of business activity (Act. No, 300/2005 of the Criminal Code, Sec.251(1) to (4); Act No.91/2016 on criminal liability of legal entities, Sec.4). Administrative fines are of a rather insignificant amount (up to EUR 3'319) and can be imposed on both, natural and legal persons.

9. **Criterion 15.6** –

(a) Some activities of VASPs covered under the FATF recommendations are not covered under the Slovak legislation (please see criterion 15.4(a)).

The other regulated types of activities of VASPs, are subject to the AML/CFT requirements (Section 5(1)(o) and (p)). The FIU is responsible for ensuring the compliance with the AML/CFT obligations (Section 26(2)(c)). The VA/VASP sectorial risk assessment conducted by FIU in March 2024 is of limited usefulness due to issues with lack of supervision, statistical data availability and complexity. There is no risk-based supervision of VASPs carried out by the FIU. Moreover, deficiencies in the VASP risk assessment negatively impact the risk-based supervision.

Also, the jurisdiction has not provided any information on the steps taken for ensuring VASPs compliance with AML/CFT requirements. The FIU made additional checks for those VASPs that did not cooperate to provide the questionnaire. The FIU Methodological Guidance on Assessment of the risk of ML/TF issued in April 2024, develops the principles for risk-based approach for all sectors, but does not set specific measures relevant for VASP sector.

(b) The FIU has the necessary powers to ensure compliance by VASPs with AML/CFT requirements (Section 29(1), Section 26(2)(c) and (e), Section 33a, Section 33(1) and (6) of the AML Act).

The deficiency identified under R.27 equally applies to VASPs, i.e., absence of the information regarding the legal processes for withdrawing, restricting or suspending the license for AML/CFT violations.

10. **Criterion 15.7** – The FIU has published a guidance document (last updated in April 2024) for VASPs and a guideline on the fulfilment of obligations under Act No. 297/2008 Coll. for legal and natural entities providing virtual currency wallet services and virtual currency exchange offices. Apart from these documents no other feedback has been provided by the authorities. AML Act Section 26(2)(i) obliges the FIU to provide feedback to the obliged persons in relation to the quality of submitted report (UTR). Nevertheless, the provision is of a general nature and refers to the procedure that the FIU shall adopt after the receipt of UTRs rather than a form of specific feedback on the quality of the UTRs and the manner in which they have been used by the FIU.

11. **Criterion 15.8** –

(a) The MER considered sanctions available for violations of terrorism & terrorism financing related TFS as not proportionate and dissuasive. Sanctions for failure to comply with other AML/CFT requirements, were not criticised. Hence, it should be noted that there is a range of proportionate and dissuasive sanctions for the failure to comply with AML/CFT requirements.

(b) No measures have been taken by Slovak Republic to impose not only on VASPs, but also to their directors and senior management.

12. **Criterion 15.9** – Covered VASPs are subjects of the AML/CFT Law and bound by the AML obligations mirroring the requirements set out in R.10-R.21. For occasional customers, VASPs are

obliged to keep all the data and written documents obtained through CDD measures and related to the transaction for 5 years after the execution of an occasional trade (AML Act, Article 19(2)). The record-keeping requirements cover risk profile assessment records, including supporting analysis, business correspondence, results of any analysis undertaken, records of all actions taken and related obstacles (AML Act, Article 19(2)(c), in relation to c.11.2). Other identified deficiencies under R.10-21 equally apply to VASPs.

(a) Covered VASPs are obliged to only identify and verify the customer identity when a trade amounts to or exceeds EUR 1 000.

(b) (i) No specific information is provided on how the country ensures travel rule requirements for VA transfers.

(ii) to (iv) Slovak Republic has not provided any relevant information that would meet the requirement of these criteria.

13. **Criterion 15.10** – Terrorism financing/proliferation financing TFS obligations apply to covered VASPs in the same manner as they apply to other obliged persons (Article 4(2)(b) International Sanctions Act 289/2016). The respective communication mechanisms and reporting obligations are provided under International Sanctions Act (Act 289/2016). However, the Ministry of Finance guidance on implementation of TFS obligations applies to financial institutions only, with no specific instructions published for other implementing entities, including VASPs (see 7.2(d)). Moreover, there is no direct reference in the legislation to "monitor" the compliance of VASPs with R.7 (see c.7.3).

14. **Criterion 15.11** – Slovak Republic was assessed as compliant with R.37 and largely compliant with R.38-R.40. Consequently, international co-operation and exchange of information can occur with a view to covered VASPs in the extent allowed by the deficiencies identified under R.38 to R.40 in the 2020 MER.

Weighting and Conclusion

15. The Slovak Republic has taken some steps to address and deficiencies under R.15 identified in the 5th round MER, however some gaps still remain. In particular, the Slovak legislation does not comply with the definition of VASP activities provided under the FATF in terms of activities such as exchange of one VA to another VA, participation in and provision of financial services related to an issuer's offer and/or sale of VA. Risk-based supervision is not conducted. The legislation does not provide a specific framework for the application of the Travel Rule. No monitoring with respect to targeted financial sanctions is applied to VASPs. **R15 remains rated PC.**

Recommendation 19 – Higher-risk countries

	Year	Rating
MER	2020	PC
FUR1	2022	PC (upgrade requested)
FUR2	2023	PC (no upgrade requested)
FUR 3	2024	PC (upgrade requested, maintained at PC)

1. In the 5th round MER, Slovak Republic was rated as PC with R.19. There were moderate shortcomings identified, including (i) applicability of enhanced customer due diligence (CDD) measures limited only to high-risk countries that are not part of the European Economic Area (EEA) area; (ii) no authorisation for competent authorities to apply countermeasures either independently or when called for by the FATF; (iii) only European Commission decisions identifying high-risk countries published by the FIU.

2. Slovak Republic requested to upgrade R. 19 in the context of the 1st FUR, however no sufficient progress has been made and the rating remained.

3. Slovak Republic has amended the AML/CFT Act to obligate the FIU to regularly update and publish on its website the list of high-risk jurisdictions with strategic deficiencies identified by FATF.

4. **Criterion 19.1** – Article 12(1) of the AML/CFT Act obliges FIs to perform enhanced CDD to a transaction or business relationship with the person established in a high-risk jurisdiction with strategic deficiencies as identified by the EU. This falls short of the FATF standard. Although the current EU list includes all those jurisdictions for which enhanced CDD measures are called for by the FATF, the relevant EU regulation (2016/1675) applies to only non-EU/EEA states. Moreover, it is unclear whether enhanced CDD measures must be applied to natural persons who reside in the high-risk jurisdiction or legal persons that primarily operate but are not formally incorporated in such a jurisdiction.

5. **Criterion 19.2** – The countermeasures that can be applied by Slovak Republic are limited to enhanced CDD measures. Other countermeasures cannot be applied either independently or when this is called for by the FATF, because it is constrained with the list of jurisdictions identified as high risk by the EU.

6. **Criterion 19.3** – According to amended Article 26(2)(o) of AML Act, FIU is publishing on its website, in addition to the decisions taken by the European Commission that identify high-risk jurisdictions with strategic deficiencies, a list of high-risk countries identified by FATF.

Weighting and Conclusion

7. There are moderate shortcomings to R.19 remaining. Enhanced CDD measures can only be applied to high-risk countries that are not part of the EEA area. Slovak Republic is not able to apply countermeasures either independently or when called for by the FATF. **R.19 remains rated PC.**

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

Recommendations	Rating	Factor(s) underlying the rating[10]
8. Non-profit organisations	PC (MER 2020) PC (FUR2 2023) **PC (FUR3 2024)**	• The authorities have identified the features and types of NPOs likely to be at risk of TF abuse to a limited extent only (c.8.1(a), as per FUR3 2024). • The sectorial risk assessment lacks thorough analysis, along with detailed threat information, failing to identify specific nature of threats posed by terrorist entities to the NPOs at risk (c.8.1(b), as per FUR3 2024). • As concerns remain under 8.1(a) criterion, it is not clear if adequacy of measures has been identified to a full extent (c.8.1(c) as per FUR3 2024). • Absence of risk-based approach in the supervision of NPOs (c.8.3).
15. New technologies	LC (MER 2020) PC (FUR1 2022) **PC (FUR3 2024)**	• There is no explicit requirement for risk assessment and mitigation to take place before launch of a new technology, product or service (c.15.2(a)(b)). • The assessment of the VA/VASP sector is constrained due to issues with lack of supervision, statistical data availability and complexity (c.15.3(a), as per FUR3 2024). • Deficiencies in relation to c.1.11 apply in relation to VASPs (c.15.3(c), as per FUR1 2022). • Not all the activities provided under the FATF definition of VASPs are covered (c.15.4(a), as per FUR1 2022). • Unclear whether the market entry requirements apply to the owner, beneficial owner, or a manager of a VASP (c.15.4 (b), as per FUR3 2024). • Criminal associates are not prevented to from holding or being beneficial owners of, a significant or controlling interest, or holding a management function in, a VASP (c.15.4(b), as per FUR1 2022). • No systemic measures are applied to identify natural or legal persons that carry out VASP activities without the requisite license or registration (c.15.5, as per FUR1 2022). • Deficiencies in the VASP risk assessment negatively impact the risk-based supervision (c.15.6(a), as per FUR1 2022). • Sanctions applicable to VASPs for violations of terrorism & TF related TFS are not proportionate and dissuasive (c.15.8(a), as per FUR1 2022). • No measures have been taken by Slovak Republic to impose not only on VASPs, but also to their directors and senior management (c.15.8(b), as per FUR1 2022). • Identified deficiencies under R.10-21 equally apply to VASPs (c.15.9(a), as per FUR1 2022). • No travel rule requirements for VA transfers

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

Recommendations	Rating	Factor(s) underlying the rating[10]
		(c.15.9(b), as per FUR1 2022). • The is no direct reference in the legislation to "monitor" the compliance of VASPs with R.7 (c.15.10, as per FUR3 2024). • International co-operation and exchange of information can occur with a view to covered VASPs in the extent allowed by the deficiencies identified under R.38 to R.40 in the 2020 MER (c.15.11, as per FUR3 2024).
19. Higher-risk countries	PC (MER 2020) PC (FUR2 2023) **PC (FUR3 2024)**	• Enhanced CDD measures can only be applied to high-risk countries that are not part of EEA area (c.19.1). • Lack of clarity whether enhanced CDD measures must be applied to natural persons who reside or legal persons what primarily operate in the high-risk jurisdictions (c.19.1). • Countermeasures (other than enhanced CDD) cannot be applied either independently or when this is called for by the FATF, because it is constrained with the list of jurisdictions identified as high risk by the EU (c.19.2).

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering/ Countering the Financing of Terrorism
BO	Beneficial owner
C	Compliant
CDD	Customer due diligence
CTU-NAKA	Counter-Terrorism Unit NAKA
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial Intelligence Unit
FUR	Follow-up report
LC	Largely compliant
LEA	Law enforcement agency
MER	Mutual evaluation report
ML	Money laundering
MoI	Ministry of Interior
NC	Non-compliant
NPO	Non-profit organisation
NRA	National risk assessment
NBAC	National Security Analytical Center
PC	Partially compliant
R.	Recommendation
SIS	Slovak Information Service
SRA	Sectorial risk assessment
TC	Technical compliance
TF	Terrorism financing
TFS	Targeted financial sanctions
UTR	Unusual Transaction Report
VA	Virtual asset
VASP	Virtual asset service provider

www.coe.int/MONEYVAL

December 2024

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Slovak Republic

3rd Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Slovak Republic's progress in addressing the technical compliance deficiencies identified in the September 2020 assessment of their measures to combat money laundering and terrorist financing and in subsequent follow-up reports.