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)19

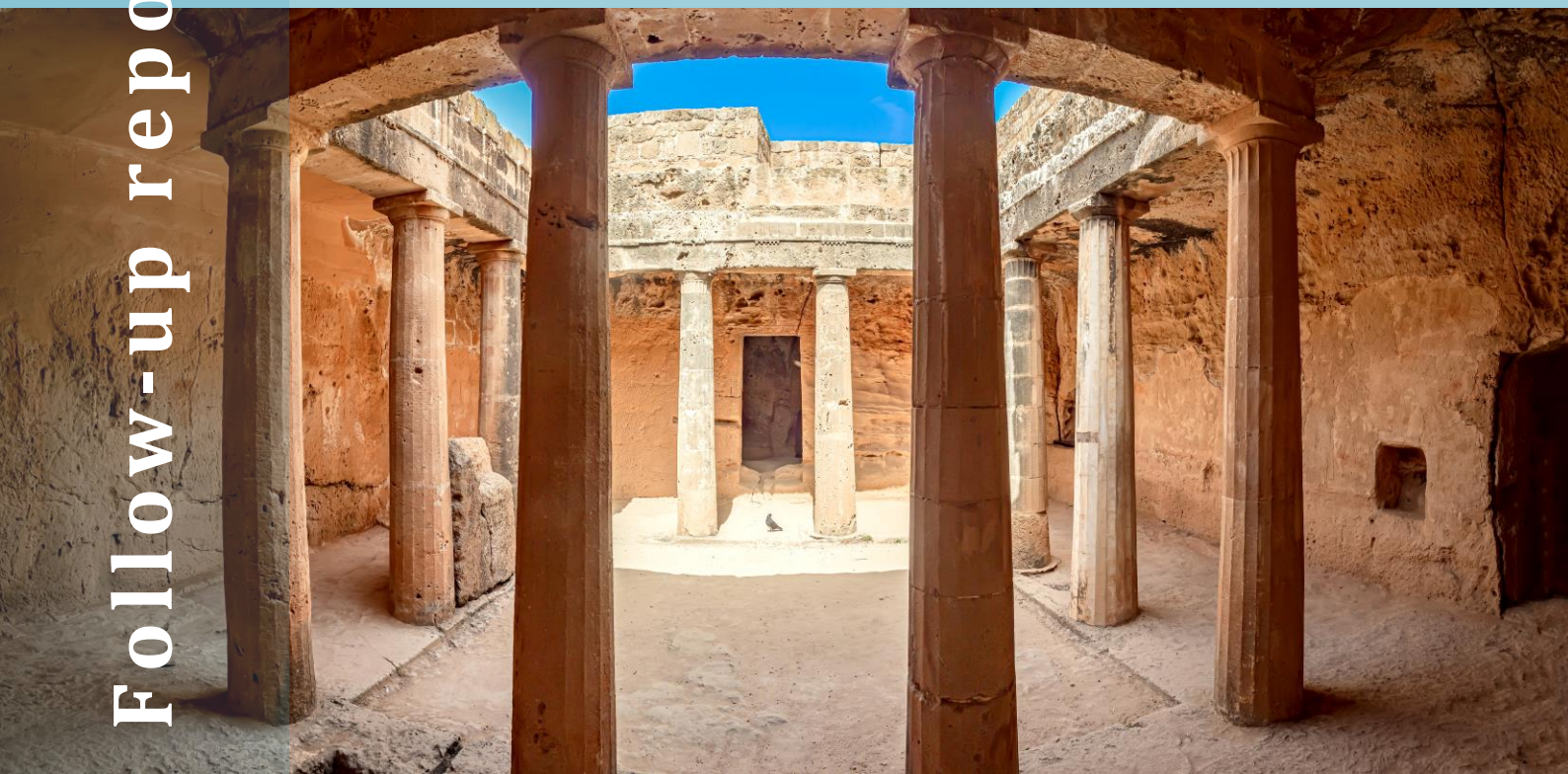
Anti-money laundering and counter-terrorist financing measures

Cyprus

3rd 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 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating on Cyprus was adopted by the MONEYVAL Committee at its 66th Plenary Meeting (Strasbourg, 14 December).

Cyprus: 3rd Enhanced Follow-up Report

I. INTRODUCTION

1. The mutual evaluation report (MER) of Cyprus was adopted in December 2019. Given the results of the MER, Cyprus was placed in enhanced follow-up.[1] Its 1st[2] and 2nd[3] enhanced follow-up reports (FUR) were adopted in December 2021 and November 2022 respectively. This report analyses the progress of Cyprus in addressing the technical compliance (TC) deficiencies identified in its MER or subsequent FURs. Re-ratings are given where sufficient progress has been made. This report also analyses progress made in implementing new requirements relating to Financial Action Task Force (FATF) Recommendations which have changed since the adoption of the 5th Round MER or applicable subsequent follow-up reports (FURs): R.15. 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 Cyprus request for technical compliance re-ratings and the preparation of this report were undertaken by the following Rapporteur teams (together with the MONEYVAL Secretariat):

- Serbia
- Slovak Republic

3. Section II of this report summarises Cyprus' progress 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 Cyprus to improve its technical compliance by:

a) addressing the technical compliance deficiencies identified in the MER and applicable subsequent FUR for which the authorities have requested a re-rating (R.8), and

b) implementing new requirements where the FATF Recommendations have changed since the MER or applicable subsequent FUR was adopted (R.15).

5. Although the authorities have requested re-ratings for R.13 and 31, currently rated partially compliant (PC), no re-ratings were considered by MONEYVAL in application of Rule 21(8) of the Rules of procedure.

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 Cyprus submitted its country reporting template, that is at least six months before the FUR is due to be considered by MONEYVAL.[4]

1. Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up involves a more intensive process of follow-up.
2. First enhanced follow-up report, available at https://rm.coe.int/moneyval-2021-20-fur-cyprus/1680a52895.
3. Second enhanced follow-up report, available https://rm.coe.int/moneyval-2022-17-fur-cy/1680a92582.
4. 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.

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

7. Whilst Cyprus has made some progress to address the technical compliance deficiencies identified in the MER and applicable subsequent FURs, it has not been re-rated in respect of FATF Recommendation 8 for which the authorities requested a re-rating.

II.2 Progress on Recommendations which have changed since adoption of the MER or applicable subsequent FUR

8. Since the adoption of Cyprus' MER, the FATF has amended R.15. Annex A provides the description of Cyprus' compliance with the new requirements, set out by criterion, with all criteria covered.

9. In the light of the progress achieved, Recommendation 15 has been re-rated from partially compliant to largely compliant.

10. It should be noted that Cyprus does not apply supervisory (c.15.6) or regulatory (c.15.9) requirements to virtual asset service providers (VASPs) that provide services on a remote basis into Cyprus from the European Economic Area (EEA) members. This exemption is stipulated as per Section 61E(2)(b) of the AML/CFT Law and is subject to sufficient evidence of the valid registration with the EEA national competent authority, before they commence their operations in Cyprus.[5] In any other cases, the EEA VASP is required to submit an application to be registered with the Cyprus Securities and Exchange Commission (CySEC). This is not treated as a deficiency since the FATF Standards, absent any assessment of higher risk, do not expressly apply such requirements to foreign VASP. The relevant criteria (15.6 and 15.9) have been assessed accordingly.

11. 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.

III. CONCLUSION

12. Overall, in light of the progress made by Cyprus since its MER, 1st and 2nd enhanced FURs was adopted, its technical compliance with the FATF Recommendations has been re-rated as follows:

Table 1. Technical compliance with re-ratings, December 2023

R.1	R.2	R.3	R.4	R.5
LC (MER)	LC (MER)	C (MER)	C (MER)	LC (MER)
R.6	R.7	R.8	R.9	R.10
LC (MER)	LC (MER)	PC (FUR3 2023) ~~PC (FUR2 2022)~~ ~~PC (FUR1 2021)~~ ~~PC (MER)~~	C (MER)	LC (MER)
R.11	R.12	R.13	R.14	R.15
C (MER)	LC (MER)	PC (FUR1 2021) ~~PC (MER)~~	C (MER)	**LC (FUR3 2023)** ~~PC (FUR2 2022)~~ ~~PC (FUR1 2021)~~ ~~LC (MER)~~
R.16	R.17	R.18	R.19	R.20
LC (MER)	C (MER)	LC (MER)	LC (MER)	C (MER)
R.21	R.22	R.23	R.24	R.25
C (MER)	LC (MER)	LC (MER)	LC (MER)	LC (MER)

5. PS-01-2021: Policy Statement on the Registration and Operations of Crypto-Asset Services Providers.

R.26	R.27	R.28	R.29	R.30
LC (MER)	C (MER)	LC (MER)	C (MER)	LC (MER)
R.31	R.32	R.33	R.34	R.35
PC (FUR2 2022) ~~PC (FUR1 2021) PC (MER)~~	LC (MER)	C (MER)	LC (MER)	C (MER)
R.36	R.37	R.38	R.39	R.40
C (MER)	LC (MER)	C (MER)	C (MER)	C (MER)

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

13. In line with Rule 21(8) of the Rules of Procedure, 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. The threshold of "most if not all addressed deficiencies" should be considered as thirty-six or more out of the forty FATF Recommendations at the LC/C level, depending on the context of the jurisdiction, but the threshold should not be lower than thirty-six, and none of the "big six" Recommendations (3, 5, 6, 10, 11 and 20) should remain NC/PC. The threshold may be adjusted upwards, depending on the context of the jurisdiction considered in conjunction with the severity of deficiencies.

14. Cyprus has currently 37 Recommendations at the LC/C level, including Recommendations 3, 5, 6, 10, 11 and 20. The Plenary concluded that Cyprus has reached the general expectation of having remedied most of the technical compliance deficiencies at the end of its 3rd year of follow-up, and that therefore the frequency of reporting may be reduced. Cyprus will remain under enhanced follow-up and is required to report back to MONEYVAL on progress to strengthen its implementation of AML/CFT measures by May 2025.

Annex A: Reassessed Recommendations

Recommendation 8 – Non-profit organisations

	Year	Rating and subsequent re-rating
MER	[2019]	[PC]
FUR1	[2021]	[PC] (upgrade requested, maintained at PC)
FUR2	[2022]	[PC] (upgrade requested, maintained at PC)
FUR3	[2023]	[PC] (upgrade requested, maintained at PC)

1. In its 2011 MER, Cyprus was rated PC with the former SR. VIII due to the absence of a comprehensive domestic review of the non-profit organisation (NPO) sector's vulnerabilities, absence of outreach to the NPO sector and deficiencies in the sanctioning regime. Since the adoption of the 2011 MER, R.8 has changed significantly.

2. **Criterion 8.1** –

(a) To address the deficiency identified in the MER for c.8.1(a), in 2023 Cyprus (with the help of an external service provider) has nearly finalised the first risk assessment of NPO sector with a view to identify a subset of NPOs which are likely to be at risk of terrorism financing (TF) abuse. The methodology used for the risk assessment encompasses multiple criteria related to money laundering (ML), TF and tax abuse. However, the risk calculation method is set up in a way to enable distinction between the indicators that are directly linked to TF risk (as opposed to ML) and thus can provide risk calculation results solely based on TF. TF risk calculation is based on the following risk indicators: negative information or sanctions applied to NPO; links of the management personnel who is a foreign politically exposed person (PEP) with high-risk countries; source of funding with a geographical component; anonymous donations, including made in cash; distribution of funds using cash or crypto assets; NPO activities (and whether the financial flows correspond to the NPO activities); country of origin of BO or trustee; maintenance of bank accounts in foreign jurisdictions; financial relations with persons from high risk countries linked to TF.

However, the NPO TF risk assessment – a formal document containing analysis and, more importantly, consolidated findings and conclusions, has not been prepared by the authorities. The authorities reported that this exercise covered 2009[6] (out of total 4151 NPOs) that fall under the FATF definition. However, non-profit companies were not included into the assessment and work on identifying non-profit companies that fall under the FATF definition has not been completed. The risk assessment results shared by the authorities show that only 2,15% NPOs assessed are exposed to a higher risk of TF abuse. The TF risk distribution is as follows: 34,39% fall under low risk; 63,46% - low to medium risk; 2,10% - medium to high risk; and the remaining 0,05% - high risk. The Cypriot authorities have shared a sanitised NPO risk calibration tool (in excel format) that highlights the TF risk level of each NPO assessed on the basis of the replies to the risk assessment questionnaire and relative importance and weighting of the assessed data points. However, information provided by Cyprus does not include a consolidated analysis of the risks that each of the above risk categories are exposed to and does not clearly emphasise the features and types of NPOs, which are likely to be at risk of TF, by virtue of their activities or characteristics.

(b) To address the deficiency identified in the MER for c.8.1(b) regarding failure to identify the nature of the threats posed by terrorist entities to those NPOs which are at higher risk (c.8.1(b)), Cyprus has identified general TF threats arising from the (i) geographical location of Cyprus;[7] (ii) NPOs' activities; (iii) governance of NPOs; and (iv) fund flows. Authorities report

6. The total number of NPOs that fall under the FATF definition differs from the total reported in the 2nd Follow-up report, where the authorities have estimated that approx. 10% (around 450) of NPOs fall under the FATF definition.
7. Since 1974, the northern part of the island has not been under Government control (occupied area).

that geographical factors might potentially influence the likelihood of fund flows towards the countries considered high risk from TF perspective. A large number of immigrants and refugees might utilise numerous fund-raising activities, including fund raising activities in cash; moreover, situations have been observed where immigrants and refugees originating from higher risk countries become members of the management bodies or beneficial owners of the NPOs, incl. those that hold PEP status in foreign jurisdictions. These threats were used as a basis to develop a list of TF risk factors which are used for the risk assessment (see c.8.1(a) for more information).

It remains unclear as to whether a TF risk assessment of the NPO sector added to the authorities' understanding of the nature of threats posed by terrorist entities to NPOs, as no formal document containing findings and conclusions has been presented for analysis. The authorities claim that Cyprus has identified specific TF threats for each NPO subjected to the TF risk assessment, however, the conclusions seem to be placed more on the risk assessment methodology, namely, the risk assessment questionnaire. Nevertheless, the authorities seem to have strengthened their understanding of the nature of TF threats through close monitoring performed on some higher risk NPOs. For example, according to the data provided by the authorities, 13 NPOs were found to be exposed to the following threats: (i) logistical support to terrorists or terrorist recruitment; (ii) raising and moving funds to support terrorists; (iii) bad governance (including poor internal controls, such as transferring money to unidentified beneficiaries or collecting money from an unidentified source). It remains unclear, however, whether the above-mentioned threats are potential, have materialised, or are suspected to have occurred.

(c) The Law on Societies and Institutions and other related matters (LSI) n was adopted in 2017 to update the legislative framework governing the activities of societies and institutions and ensuring that it is in line with the requirements under R.8. The authorities have clarified that most charities in Cyprus are state-funded and therefore they are unlikely to pose a high risk for TF, therefore remain governed under the Charities Law. Cyprus initiated a review of the adequacy of the measures that apply to non-profit companies. Authorities report that the decision has been taken to establish an Ad Hoc Committee that is tasked with reviewing the control framework for non-profit companies and suggesting necessary changes to it, if deemed necessary. The authorities report that the review has been finalised and relevant drafts amending legislation have been prepared, however, the results of such a review have not been shared by Cyprus. As noted under c.8.1(a), non-profit companies are still to be assessed for TF risk which is pre-requisite for such a review.

No actions have been taken to review the current legal and regulatory framework for the entire subset of NPOs aimed at assessing as to whether or not legal and regulatory requirements proportionately and effectively target varying levels of TF risk exposure by all NPOs falling under the FATF definition.

(d) In 2023 Cypriot authorities nearly completed the first TF risk assessment of the NPO sector (see c.8.1(a) for more information and the shortcomings identified). According to the authorities, the TF risk assessment of the NPO sector should be revised every 5 years.

3. **Criterion 8.2** –

(a) Currently, the same requirements apply to non-profit companies as to regular companies. Non-profit companies are required to file annual returns, prepare financial statements in line with the International Accounting Standards, and can be subject to the strike off procedure (Art. 119, 121, 142 of the Companies Law). For every company that is required to prepare consolidated financial statements, mandatory audit or review of the financial statements, consolidated financial statements, management report and consolidated management report by auditors is required (Art. 152A(1) of the Law on Companies). These requirements provide a level of accountability in the administration of non-profit companies; however, additional

measures are expected to promote integrity and public confidence in the administration and management of non-profit companies. As noted at c.8.1(c), although the authorities stated that the review of the adequacy of the measures in relation to non-profit companies has been finalised, no relevant documents on the results thereof have been shared. Moreover, non-profit companies were not part of NPO risk assessment thus it is not clear on which basis the review has been conducted and legislative changes prepared, as announced by the authorities.

(b) Extensive outreach was conducted to the NPOs by approx. mid-2022 on different topics, such as risks to the NPO sector, self-monitoring, best practices, etc. However, the scope and depth of the discussed topics that relate to risks and vulnerabilities cannot be fully determined, as only partial translations into English of the training material were made available. Outreach events were attended by the representatives of approx. 1,000 NPOs (out of approx. 4,500). No differentiation was made between different types of NPOs when designing the content of training/outreach material, thus it is doubtful whether the scope and depth of the outreach was determined on the risk sensitive basis and/or carefully considered different characteristics of NPOs. Although no specific TF-related educational programmes have been designed for the donor community, however, Cyprus authorities report the existence of outreach events, i.e., the President of the Donation's Authority speaks regularly (once every three months) on TV and radio channels about various fundraising activities, including protection from TF abuse.

    In 2023, the authorities reported that they continue to conduct outreach to "umbrella" NPOs that focuses on communication of good practices guidance, governance, legal framework and implementation challenges thereof, monitoring by the competent authorities and unintended consequences. Although generally these topics deserve attention by both, NPOs and the authorities, the themes discussed, however, do not specifically cover potential vulnerabilities of NPOs to TF abuse and TF risks and the mitigating measures that NPOs can undertake to protect themselves from TF abuse. The Communications Strategy outlines the mechanisms for communication between relevant government authorities and the NPO sector in order to raise awareness on these issues. However, a brief summary of the training material does not support that TF aspect is appropriately covered in the outreach activities.

(c) The Ministry of Interior published a guidance for the sound operation of NPOs (best practices paper). This guidance – designed to be used as a self-diagnostic tool – covers key areas necessary to protect NPOs from TF abuse. The best practices paper, however, concentrates on discussing governance, internal control and operational principles rather than focusing on the protection from TF abuse in depth. For example, the guidance paper further suggests that resources can't be transferred to the persons involved in gambling but is silent regarding any other beneficiary-related risk factors which might be more indicative of TF risk, such as targeted financial sanctions' screening performed on beneficiaries, including residence in high-risk areas or conflict zones, etc. Moreover, it is not clear as to why donating money is considered a higher risk for TF than sending money to beneficiaries, as no such geographical restrictions for beneficiaries exist as opposed to restrictions for donors, etc. In addition, the best practices paper is uniform and does not differentiate between varying levels of risk exposure by NPOs, nor different types, features and characteristics of NPOs (which, in turn, should signal different types of vulnerabilities). As a result, some requirements contained in the best practices paper seem to place excessive burden to NPOs that are lower risk and/or have limited capacity to adhere to the best practices (e.g., due to small size/scope of the activities), which, consequently, can potentially discourage legitimate NPO activities. Authorities admit that the NPO community expressed diverging views concerning the requirements of the best practices – some welcomed the paper and suggested additional risk-linked amendments, some – were more critical (to support this, specific examples of the feedback from the NPO community were provided by the authorities). Communication with the NPO community is ongoing after the issuance of the best practices paper.

The Cypriot authorities are considering development of more targeted guidance ("best practice") paper that takes into account different types, features and characteristics of NPOs as well as varying levels of risk exposure of NPOs.

(d) The best practices paper issued by the Ministry of Interior promotes usage of the banking system.

4. **Criterion 8.3** – Cyprus is making further progress towards addressing the deficiencies identified in the MER for c.8.3. The authorities developed a risk-based monitoring methodology (Risk Based Approach for the monitoring of Money Laundering and Terrorism Financing Risks in the NPO sector) and a monitoring strategy. Two types of monitoring are relevant here: (i) basic monitoring and (ii) close monitoring performed by the Ministry of the Interior. As an additional tool, the risk-based monitoring methodology also foresees possibility for thematic reviews that can be performed on a case-by-case basis, dependent on the trigger events or other similar circumstances. Authorities report that basic monitoring is performed yearly (desk-based review) and is based on the following criteria: financial information, activities, beneficial ownership screening, screening regarding maintenance of local bank accounts and risk questionnaire. According to the risk-based monitoring methodology, close monitoring is informed by the outcomes of the risk assessment of the whole NPO sector, i.e., frequency of the close monitoring actions will be dependent on the risk level of the individual NPOs. However, the risk-based monitoring methodology does not discuss in detail (i) whether scope and depth of the monitoring is being determined based on the TF risk profile; (ii) certain elements that are of key importance to prevent TF abuse of NPOs, such as, controls relating to the funds transfer to beneficiaries, incl. TF-related targeted financial sanctions screening, etc. Moreover, the aforementioned methodology encompasses not only the risk elements of TF, but also ML. Consequently, risk-based actions might not be solely based on TF, but also ML. However, the authorities reported that more concrete methodology for close monitoring is yet to be developed. Positive actions are being taken by the authorities to build capacity of the teams that are tasked with the close monitoring function, such as trainings aimed at deepening the understanding of the financial statements and accounting principles, as well as ongoing discussions on TF risks.

5. Since the second Follow-up report, the TF risk categorisation of NPOs allowed the authorities to advance their risk-based monitoring approach, i.e., a risk matrix is used for determining the scope and frequency of supervision of NPOs in accordance with its risk level and the authorities were able to share some information on the most relevant supervisory findings and actions to be taken, based on those findings.

6. **Criterion 8.4** –

(a) *Societies, institutions, federations/associations, charities:* The implementation of the requirements under the LSI is monitored by the General Registrar (and District Registrars) within the Ministry of Interior. Monitoring is conducted off-site on the basis of information (e.g. mandatory notifications, audited financial statements) submitted by the NPOs to the registrar. With respect to societies only, the General and District Registrars may carry out inspections, acting on a complaint or on their own initiative, to ascertain whether the conditions laid down in the LSI are fulfilled (Art.7(6)). In addition, the registrar or any person who may establish a legitimate interest may go to the court and request the issue of an order for auditing the accounts of a society, institution or federation/association. The auditing is carried out by the Auditor General.

Non-profit companies are registered with the Department of Registrar of Companies and Official Receiver and have an obligation to file changes and annual return forms.

(b) Article 4 of the LSI provides that societies, institutions or federations/associations that are unlawful in the meaning of Article 63 of the Criminal Code (unlawful association) or the object or operation of which aims or tends to undermine the Republic, the democratic institutions, the security of the Republic, the public interests, the fundamental rights and freedoms of all persons, shall have no legal existence, and should be either refused registration, or dissolved by order of the Court. Additionally, any person who is a member of

the unlawful society, institution or federation/association, shall be guilty of an offence and liable to imprisonment not exceeding three (3) years or a fine not exceeding EUR 3,000 or to both such penalties.

To address the deficiency identified in the MER for c.8.4(b), Cyprus has amended "Associations and Foundations and other related matters Law", however, sanctions foreseen in this law do not apply to charities (regulated by Charities Law) and Non-profit companies. As noted in the second Follow-up-Report, a large number (2,446) of NPOs registered under the previous Societies and Institutions Law of 1972 have been deleted from the register for non-compliance reasons. As a result, these NPOs have lost their legal ability to operate, and their property has been alienated. In particular, their bank accounts were frozen. Reasons for removal have included anomalies with funding and in the preparation of financial statements. Although the particular scope of sanctions for breaching the Societies and Institutions Law is limited to striking from the register and dissolution, this is considered to be an important sanction. However, extensive de-registration raises a question as to whether or not there have been unintended consequences. The authorities reported that charities and non-profit companies can be also struck off from the register.

All legal persons, including NPOs can be sanctioned for non-provision of information concerning beneficial owners (AML/CFT Law, Art. 61(b)(10)): NPOs can be subject to a fine of EUR 200 and an additional fine of EUR 100 for each day for which the breach is continued, with a maximum fine of EUR 20,000. If an NPO provides misleading or false information, it can be subject to EUR 100,000 fine or subject to a term of imprisonment of no more than one year; these sanctions are also applicable to NPOs' controllers (AML/CFT Law, Art. 61(b)(10)(g)). The authorities reported that 592 NPOs have received warning letters with respect to failure to submit financial statements and information on beneficial owners and controllers. In addition, on the basis of the Companies Law (also applicable to the NPOs), fines can be applied for non-submission of information concerning registered office (Art. 102), directors and company secretary (Art. 192), shareholders (Art. 113A), annual return form (Art.120).

Upon completion of the TF risk assessment of the NPO sector, Cyprus should carry out an overall review of the adequacy of legal and regulatory measures to address the identified risks. Consequently, this review would be key to assess effectiveness, proportionality and dissuasiveness of sanctions for NPOs or their controllers.

7. **Criterion 8.5** –

(a) Information on societies, institutions and federations/associations is held by the General Registrar and the District Registrars. There are effective systems in place to ensure cooperation, coordination and information sharing between them. Information on charities and non-profit companies is held centrally by the Tax Authority and the Ministry of Energy, Commerce and Industry respectively. There are no other authorities which hold relevant information on NPOs within Cyprus.

(b) It is doubtful that there is any investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations. In 2020-2021, 4 cases were opened and still under investigation by law enforcement agencies (LEAs) which involved NPOs. None of these cases are specifically related to investigations related to misuse of NPOs to support terrorist activities or organisations.

The authorities have not provided concrete evidence that the investigative expertise and capability of the authorities to examine NPOs suspected of TF involvement has increased, however, the authorities reported that the Police is constantly increasing its knowledge on the TF aspect through trainings and participation in international fora.

(c) The LSI and the Charities Law require NPOs to submit information on their administration and management, which information is maintained by the respective registrars. This

information is available to all competent authorities during the course of an investigation on the basis of the powers described under Rec. 31.

(d) There is no specific mechanism to ensure that, when there is a TF suspicion involving an NPO, information is shared promptly with the competent authorities. Registry staff are expected to report to the police, the Financial Intelligence Unit (FIU) or Auditor General where risk factors are identified. The Cyprus police demonstrated that they cooperated with several NPOs under suspicion, however this is not considered a mechanism for the prompt sharing of information.

Nevertheless, the authorities stated that they would rely on a risk assessment and an oversight mechanism over NPOs during which, if suspicion arises, an official of the Ministry of Interior is responsible for sharing this information with the law enforcement authorities. Although this is positive, it does not amount to a specific mechanism for information sharing on TF suspicion involving NPOs. There does not seem to be a mechanism for prompt information sharing such as cooperation agreements between authorities, liaison officers, a specific task force or similar arrangements.

8. **Criterion 8.6** – International requests involving NPOs, if they had to arise, would be received either through the formal channels (i.e. the Ministry of Justice and Public Order) or informally by the Police or the FIU. The Police and the FIU would obtain the requested information from the General/District Registrar. However, there are no points of contact or procedures specific to requests related to NPOs suspected of TF or other forms of terrorist support.

9. The deficiency with regard to criterion 8.6 remains. There are no points of contact and procedures to respond to international requests concerning NPOs suspected of TF involvement.

Weighting and Conclusion

10. Cyprus has taken a number of measures in respect of NPOs, however, a number of shortcomings remain: (i) a formalised document on TF risk assessment of the NPO sector containing analysis and conclusions on risks and threats pertaining to NPO sector is absent, however, the authorities were able to provide a risk categorisation matrix and anonymised replies to a risk assessment questionnaire; the risk assessment does not cover non- profit companies (c.8.1a); the re-assessment of risk has hence not commenced, it is planned to be updated every 5 years c.8.1(d); (ii) outreach and educational awareness programs need to be better targeted and focused on TF threats, vulnerabilities and actions aimed at protection from TF abuse (c.8.2(b)); (iii) Best practices guidance would benefit from extending the scope of requirements that would be indicative of TF risks/threats; there needs to be closer cooperation with the NPO community regarding development of best practices aimed at protecting from TF abuse (c.8.2(c)); (iv) although good progress has been made towards ensuring risk-based monitoring of NPOs, further advancement is needed (c.8.3); (v) no additional legislative changes are introduced relating to sanctions for non-compliance with the requirements under R.8 (c.8.4(b)); (vi) Cyprus has not demonstrated that LEAs and other competent authorities possess specific investigative expertise and capability to examine NPOs exploited for terrorist activities or by terrorist organisations (c.8.5(b)); (vii) there is no specific mechanism to ensure that information related to TF suspicion involving an NPO is shared promptly with the competent authorities (c.8.5(d)); (viii) there are no points of contact or procedures specific to requests related to NPOs suspected of TF or other forms of terrorist support (c.8.6); and (ix) deficiencies identified in the MER concerning non-profit companies remain, namely, lack of evidence of a completion of review process concerning the adequacy of measures (and its results)(c.8.1(c)) and lack of measures to promote accountability, integrity and public confidence in administration and management(c.8.2(a)). **Cyprus remains rated partially compliant in respect of R.8.**

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	[2019]	[LC]
FUR1	[2021]	[PC] (re-rated to PC)
FUR2	[2022]	[PC] (upgrade requested, maintained at PC)
FUR3	[2023]	[↑ LC] (upgrade requested, re-rated to LC)

11. In the 2011 MER, Cyprus was rated largely compliant with the equivalent Recommendation under the 2004 FATF methodology. The deficiency noted was that there were no provisions regarding misuse of technological developments. The revised R.15 focuses on the assessment of risks related to the use of new technologies, in general, and caters for a comprehensive set of requirements in relation to VASPs.

12. The definition of crypto-asset service provider ("CASP") under Article 2(1) of the AML/CFT Act covers all of the five activities of the FATF definition of VASP. CASPs are obliged entities subject to AML/CFT obligations in terms of the AML/CFT Act under the supervision of CySEC. The term "crypto asset" (CA) is defined under the same article and is consistent with the FATF definition of virtual assets (VA).

13. **Criterion 15.1** – Section 66(2A) of the AML/CFT Act requires all obliged entities to identify and assess ML/TF risks before promoting any new technology, service or product. While the meaning of "promoting" is not entirely clear it is considered to cover development. This requirement does not cover new business practices and developing technologies and neither does it specify that the assessment of risk of technology should cover its application to both new and pre-existing products. However, obliged entities are all under an indirect obligation to identify and assess the ML/TF risks that may arise in relation to new technologies. They are required to undertake enhanced customer due diligence in situations that present a high risk of ML/TF, and in assessing situations that pose high risks they are also required to consider, among others, "new business practices and the use of developing technologies for both new and pre-existing products", AML/CFT Law, Sec. 64(3) and Annex III, para. 2(e). There have been no legislative or technical changes adopted that will mitigate the deficiencies present in this criterion, however it is noted that a future change in legislation is proposed.[8]

14. **Criterion 15.2** –

(a) Section 66(2A) of the AML/CFT Act requires obliged entities to identify and assess the risk of ML/TF prior to promoting any new technology, service or product. For credit institutions, the risk assessment must be conducted prior to the launch of the new products, business practices or the use of new or developing technologies (section 13 of the Central Bank of Cyprus (CBC) directive).

(b) Credit institutions must take measures to manage and mitigate such risks (section 13 of the CBC directive). Entities regulated by CySEC must specifically undertake "measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for money laundering and terrorist financing" (CySEC AML/CFT Directive, para. 9(1)(a)). Other obliged entities more generally must take measures to prevent the use of products or transactions that may favour anonymity and must apply reasonable measures and procedures to address the risks of technological developments and new financial products (AML/CFT Law Sec. 66(3)). This obligation does not clearly extend to new business practices in general, or to new delivery mechanisms in particular. Apart from the enhanced customer due diligence requirements under Sec. 64(3) of AML/CFT Law, there are no more detailed requirements for insurance firms, payment institutions, for e-money institutions, credit acquiring companies, bureaux de change to manage and mitigate these risks. However,

8. Legislation adopted on 20/10/2023 (outside of the scope of the assessment period) has not been assessed in this FUR.

these sectors are not material in Cyprus. There have been no legislative changes adopted to mitigate the deficiencies present in this criterion.

15. **Criterion 15.3** –

(a) Cyprus has commissioned a specific NRA on ML/TF Risks on VA and VASP activities ("VASP NRA") and published this in December 2021. The VASP NRA is very comprehensive and provides an honest analysis, using various inputs, into the threats, vulnerabilities, and structural weaknesses in VAs and VASP activities in Cyprus, but does not fully enumerate the size (in particular number and volume of transactions conducted by financial institutions (FIs) that conduct VA activities) and nature of trading in VAs by investment firms (four in total) and their corresponding threats. However, risks linked to trading in VAs by investment firms appear to be understood and the NRA indicates that VAs form a negligible part of the overall volume of these firms' activities. The VASP NRA identifies structural and capability weaknesses in the Cypriot system and makes recommendations to address these weaknesses.

To increase understanding of VA related activities, CySEC have conducted work to collect risk and statistical information from the CASPs registered in 2022. This includes the trading in VAs undertaken by investment firms. Conclusions that have been drawn so far relate to the number of customers, the volume of transactions and the income derived from this activity within the investment firms that are offering this business and therefore mitigate the deficiencies identified in the previous FURs. The findings of the information obtained as part of the project support the conclusions of the NRA.

In relation to VASPs registered in the EEA providing services to Cyprus under the AML/CFT Law, Art. 61E(2)(b), the authorities mitigate the risks by ensuring that the VASP is registered with one or more EEA national competent authorities for AML/CFT purposes; where services cannot be evidenced, the VASP must submit an application to be registered with CySEC (AML/CFT Law, Art. 61E). CySEC lists the relevant EEA VASPs on their website and ongoing media monitoring by CySEC in respect of those listed is performed.

(b) CySEC has developed an action plan to address risks identified in the risk assessment, which involves taking action to: (i) update and refine its risk-based supervisory framework; (ii) train its staff; (iii) recruit additional staff; and (iv) detect unauthorised activity. It has also placed limits on VA activities of FIs and is using specialised blockchain tools to assist with authorisation and ongoing supervision. The FIU and the Cyprus Police are also taking actions to enhance the analysis and investigation of VA related ML. The previous follow-up report noted that there is however no national action plan.

To mitigate this deficiency, Cyprus has adopted a National Action Plan based on their understanding of their risks in the NRA. This action plan consists of 66 points to be addressed that relate to VAs and VASPs, actions that are proposed and have been undertaken, the competent authorities responsible and the planned timeframes.

(c) Covered CASPs (see 15.4(a) and 15.6(a)) are required to apply risk mitigation measures in line with c.1.10 and c.1.11 being rated as met in the 2019 MER.

16. **Criterion 15.4** – Cyprus introduced a registration regime for CASPs, however, some deficiencies have been identified in connection with this registration regime.

(a) In terms of Section 61(E) of the AML/CFT Law CASPs are required to register with the Register of CASPs maintained by CySEC, when (i) providing or carrying out services or activities on a professional basis from Cyprus, regardless of their registration in a Member State's register for the services or activities they provide; (ii) providing services or carrying out activities on a professional basis in Cyprus, with the exception of persons providing crypto-asset related services or activities in Cyprus who are registered in a Member State's register for the services or activities they provide. It is however not clear that every legal

person created in the jurisdiction (whether or not it offers VA services from Cyprus) is required to register as a CASP in Cyprus as set out under c.15.4(a)(i). There have been no legislative changes adopted that will mitigate the deficiencies present in criterion 15.4(a), however it is noted that a future change in legislation is proposed.[9]

(b) Section 61E(10) of the AML/CFT Law requires the CySEC to evaluate - on an ongoing basis - the "competency and honesty" of persons who are "beneficiaries" in a VASP. Paragraph 6(1)(d) of the CASP Registration Directive requires "beneficiaries of CASPs" to be honest and competent, "which is fulfilled if they have a good reputation and the ability to maintain the strong financial position of CASP." Section 2 of the AML/CFT Law defines what is meant by a CASP beneficiary which, when read with the definition of "qualifying holding", covers both direct, indirect, and significant interests in a CASP - as provided for in the methodology. The term "good reputation" for the purposes of 6(1)(d) is defined in paragraph 6(1)(b)(i) of the CASP Registration Directive and includes a conviction for a "relevant offence". The list of offences is not considered to be sufficiently wide, although uncovered offences such as drug or human trafficking could be taken into account by CySEC when considering integrity, since any relevant factor can be taken into account. The same provisions apply to associates of beneficiaries and to those holding a management position (via paragraphs 6(1)(d) and 6(1)(b) of the CASP Registration Directive). There have been no legislative changes adopted that will mitigate the deficiencies present in criterion 15.4(b), however, it is noted that a future change in legislation is proposed.

17. **Criterion 15.5** – Section 61(E) of the AML/CFT Law requires the registration of CASPs (see c.15.4 above). CySEC explained that it takes a number of actions to identify those who may be acting outside of the registration requirements. These include following up complaints, use of internet searches and media monitoring. Section 37(1) of the CySEC Law sets the right to impose an administrative fine on any person that acts in violation of any provisions of the AML/CFT Law. The term 'person' is defined in CySEC's Law, as 'any legal or natural person and hence CySEC may impose administrative fines not only to regulated entities, but any natural or legal person including one conducting unauthorised business. A sufficient range of fines can be imposed for breaches of the registration requirement which include administrative fines not exceeding EUR 350,000 and in case of repeated violation EUR 700,000. Where illicit gain is made exceeding these latter amounts the CySEC may impose a fine of up to double the amount of the illegal gain (Law regulating CySEC, Art. 37(1) and (2)). CySEC is also empowered to require the cessation of the unauthorised activities (Law regulating CySEC Art. 25(1)(o)). It is noted that one of the recommended actions of the VASP NRA is that "Cyprus should consider whether to establish criminal liability by statute for failure to register as a VASP". There have been no legislative changes adopted since the previous FURs that will mitigate the deficiencies present in criterion, however it is noted that a future change in legislation is proposed.[10]

18. **Criterion 15.6** –

a) By virtue of Section 2A(i) of the AML/CFT Act, CASPs registered under Section 61(E)(1) are subject to AML/CFT regulation and supervision. Supervisory authorities are required to "base the frequency and intensity of the on-site and off-site supervision on the risk profile of obliged entities, and on the ML/TF risks in Cyprus.
b) CySEC has the same powers available to supervise covered VASPs as it has for other obliged entities. These have been assessed under R. 27 (rated as compliant).

19. **Criterion 15.7** – Previous reports found that guidance on identifying TF suspicion is limited and guidance issued is referencing FATF Guidance and does not provide guidance on the identification of TF suspicions in the context of VASPs in Cyprus.

9. Legislation adopted on 20/10/2023 (outside of the scope of the assessment period) has not been assessed in this FUR.
10. Legislation adopted on 20/10/2023 (outside of the scope of the assessment period) has not been assessed in this FUR.

20. This deficiency has been mitigated as CySEC has published (on June 1, 2023) *Guidance on identifying, assessing and understanding Terrorist Financing risks in the context of Crypto assets activities*. The guidance is comprehensive and covers CA vulnerabilities and risks, transactions monitoring and customer due diligence (CDD), detecting and reporting suspicious transactions, red flag indicators and employee education and training.

21. ***Criterion 15.8*** –

(a) Section 59(6) of the AML/CFT Act empowers the CySEC to take a number of regulatory actions including imposition of fines up to EUR 1,000,000, the modification, suspension and revocation of its authorisations, prohibition on persons performing administrative duties, the application of administrative penalties to natural persons as well as naming and shaming powers. In addition to these administrative sanctions, criminal sanctions are applicable in some circumstances (reporting and tipping off). These sanctions are in line with those applicable to other obliged entities, assessed as compliant under R.35.

(b) Section 59(6)(v) of the AML/CFT Act gives the supervisory authority power to impose administrative fines on natural persons if this was a result of that person's fault, intentional omission or negligence. These sanctions are in line with those applicable to other obliged entities, assessed as compliant R.35.

22. ***Criterion 15.9*** – The AML/CFT Act applies only to covered CASPs[11] (see shortcomings in coverage outlined in c.15.4(a) and c.15.6(a)) that are registered (Section 2A(i) of the AML/CFT Act), hence CASPs that fail to register are not required to apply preventive measures. Moreover, deficiencies identified in R.13, R.16 and R.18 impact the implementation of this criterion.

(a) Section 60 of the AML/CFT Act applies CDD measures to covered CASPs in the same way as for FIs except that the threshold on occasional VA transactions is EUR 1,000 or above (Section 60(g) of the AML/CFT Act). There have been no legislative changes adopted since the previous FURs that will mitigate the deficiencies present in criterion 15.9(a), however it is noted that a future change in legislation is proposed.

(b) (i) There is no requirement envisaged through enforceable means requiring originating VASPs to submit immediately and securely with a VA transfer originator and beneficiary information and (ii) some required originator and beneficiary information may not be held since (unlike under R.16) there is no obligation to obtain it. Also, the authorities have not explained whether the originating VASP is required to make information held available on request to the authorities. (iii) There are no requirements placed on the beneficiary VASP to monitor transfers lacking required information. Given that Section 2 of the AML/CFT Law includes crypto assets in the definition of "property", the powers available under the AML/CFT Law apply to crypto assets in the same way as other types of property. In respect of designated persons under UNSCRs, the authorities explain that the definition of "property" under the Combating of Terrorism and Victims' Protection Law is similar to the AML/CFT Law. The former law covers the freezing of property relating to designated persons by covered VASPs. (iv) The obligations envisaged under c.15.9(b) do not apply to FIs when sending or receiving VAs on behalf of a customer. R.18 in the MER states that there is no general, universal requirement for independent audit in obliged entities, which equally applies to CASPs, and is therefore a deficiency under this criterion. There have been no legislative changes adopted since the previous FURs that will mitigate the deficiencies present in criterion 15.9(b).

23. ***Criterion 15.10*** – All 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), also apply to covered CASPs as obliged entities under the AML/CFT Law. Only minor shortcomings have been identified.

11. Refer to paragraph 10 for rating explanation.

24. ***Criterion 15.11*** – The cooperation mechanisms available to competent authorities in respect of crypto-assets and covered CASPs are the same as for all other activities covered by the AML/CFT Law. However, the ability to use specific powers envisaged under R.31 also within the scope of international cooperation are hampered by the fact that the circumstances in which interception of the content of communications is allowed is limited to a number of offences listed in the constitution, which does not include ML or TF, or all predicate offences linked thereto.

25. There have been no legislative changes adopted since the previous FURs that will mitigate the deficiencies present in criterion.

Weighting and Conclusion

26. Cyprus has made clear progress towards improving the key deficiencies in R15, particularly by adopting and undertaking a National Action Plan which demonstrates a commitment to improving the situation relating to VAs and VASPs as well as the issuance of a Guidance document for TF in CAs. The following minor shortcomings remain: (i) the lack of requirement to identify and assess risk that may arise in relation to new business practices or developing technologies (c.15.1); (ii) it remains not clear that every legal person created in Cyprus will be required to register as a VASP in Cyprus (c.15.4); (iii) some gaps in relation to the application of fit and proper measures (c.15.4); (iv) insufficient sanctions (c.15.5) and preventive measures for failure to register as required (c.15.9); and (v) deficiencies under R. 13, 16, 18 and 31 that have an impact on R.15. **Therefore, R.15 is re-rated as largely compliant.**

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

Recommendations	Rating	Factor(s) underlying the rating[12]
8. Non-profit organisations	PC (MER 2019) PC (FUR1 2021) PC (FUR2 2022) PC (FUR3 2023)	• Cyprus has identified the subset of NPOs which may be vulnerable to TF abuse but has not issued a formalised document containing risk analysis and conclusions pertaining to NPO sector; the risk assessment does not cover non-profit companies (c.8.1(a)). • Cyprus has identified the nature of general threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs, however, it is not clear whether the NPO risk assessment has informed authorities in depth understanding of TF threats (c.8.1(b)). • There has been no review of the adequacy of measures (including laws and regulations) related to non-profit companies (c.8.1(c)). Although authorities claim that the review was finalised, the outcomes and results of this process has not been shared. • Not clear whether any measures have been taken to promote accountability, integrity and public confidence in the administration and management of non-profit companies (c.8.2(a)). • Outreach on the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse has to be deepened (c.8.2(b)). • Although good progress has been made towards ensuring risk-based monitoring of NPOs, further advancement is needed (c.8.3). • Best practices paper concentrates on discussing governance, internal control and operational principles rather than focusing in depth on protection from TF abuse (c.8.2(c)). • It is doubtful that there is any investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations (c.8.5(b)).

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

		• There is no specific mechanism to ensure that, when there is a TF suspicion involving an NPO, information is shared promptly with competent authorities (c.8.5(d)). • There are no points of contact or procedures specific to requests related to NPOs suspected of TF or other forms of terrorist support (c.8.6).
15. New technologies	LC (MER 2019) PC (FUR1 2021) PC (FUR2 2022) LC (FUR3 2023)	• There is explicit requirement to identify and assess risk that may arise in relation to new business practices or developing technologies (c.15.1-c.15.2). • It is not clear that every legal person created in Cyprus will be required to register as a VASP in Cyprus (c.15.4a(i)). • Some gaps in relation to the application of fit and proper measures under the AML/CFT law remain. This since holders or beneficial owners of significant or controlling interest in VASPs are required to have a good reputation, and the list of criminal offences linked to the term "good reputation" is not sufficiently wide (c.15.4(b)). • It is not clear that a sufficient range of sanctions can be applied to more serious breaches of registration requirements. (c.15.5). • Preventive measures do not apply to VASPs that fail to register as required (c.15.9). • The deficiencies under Recommendations 13, 16 and 18 have an effect on R.15 (c.15.9). • Court orders allowing for the actual interception of the content of communications do not extend to the investigation of ML, associated predicate offences and TF (linked to R.37 and R.31) (c.15.11).

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering and combating financing of terrorism
BO	Beneficial owner/beneficial ownership
C	Compliant
CBC	Central Bank of Cyprus
CDD	Customer due diligence
CA	Crypto Assets
CASP	Crypto asset service provider
CySEC	Cyprus Securities and Exchange Commission
EDD	Enhanced customer due diligence
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FUR	Follow-up report
FIs	Financial institutions
FIU	Financial Intelligence Unit
LC	Largely compliant
LEA	Law enforcement agency
LSI	The Law on Societies and Institutions and other related Matters Law
MER	Mutual evaluation report
ML	Money laundering
NC	Non-compliant
NPO	Non-profit organisation
NRA	National Risk assessment
PC	Partially compliant
PEP	Politically Exposed Person
SR	Special Recommendation
TC	Technical compliance
TF	Terrorism financing
VA	Virtual assets
VASP	Virtual Asset Service Provider

www.coe.int/MONEYVAL

December 2023

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Cyprus

3rd Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Cyprus's progress in addressing the technical compliance deficiencies identified in the December 2019 assessment of their measures to combat money laundering and terrorist financing.

The report also looks at whether Cyprus has implemented new measures to meet the requirements of FATF Recommendations that changed since the 2019 assessment.