COUNCIL OF EUROPE'S 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(2025)22

Anti-money laundering and counter-terrorist financing measures

Estonia

2nd Enhanced Follow-up Report & Technical Compliance Re-Rating

September 2025

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 2nd Enhanced Follow-up Report and Technical Compliance Re-Rating on Estonia was adopted by the MONEYVAL Committee through written procedure (29 September 2025).

Estonia: 2nd Enhanced Follow-up Report

I. INTRODUCTION

1. The 5th round mutual evaluation report (MER)[1] of Estonia was adopted in December 2022. Given the results of the MER, Estonia was placed in enhanced follow-up[2] and its 1st enhanced follow-up report (FUR)[3] was adopted in December 2024. This report analyses the progress of Estonia in addressing the technical compliance (TC) deficiencies identified in its MER and/or subsequent FUR, where requested to do so by the country. 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.[4]

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

- Isle of Man.

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

4. In line with MONEYVAL's Rules of Procedure, the follow-up process is desk-based – using information provided by the authorities, including revised legislation. It does not address what progress a country has made to improve the effectiveness of changes introduced by the country.

II. BACKGROUND, RISK AND CONTEXT

5. A number of significant changes have been made since adoption of the MER or subsequent FUR that are relevant for considering Recommendations that have been reassessed.

6. Since the last follow-up report Estonia has passed the Market in Crypto-Assets Act (MCAA) which came into force on the 1st of July 2024.[5] The MCAA regulates the activities, liability, dissolution and supervision of a participant in markets in crypto assets, elaborating and supplementing the provisions contained in regulation (EU) 2023/1114 and regulation (EU) 2022/2554.

7. To implement the requirements of the EU Regulation 2023/1114 on markets in crypto-assets and the EU Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets, Estonia has passed amendments to the Money Laundering and Terrorist Financing Prevention act (MLTFPA),[6] which came into effect in December 2024. As at 02 May 2022, there were 369 valid licenses in issue.

8. Since the 1st of January 2025 the EFSA is responsible for authorisation and both financial and AML/CFT/TFS supervision of crypto-asset service providers (CASPs) pursuant to EU Regulation 2023/1114 and national (MCAA) legislation. There have been no CASP licenses issued by the EFSA yet. The existing virtual asset service providers (VASPs) – 39 as of May 2025,[7] are allowed to provide

1. Mutual Evaluation Report 2022 available at https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96.
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 Follow-up Report available at https://rm.coe.int/moneyval-2024-23-estonia-5thround-1st-fur/1680b34ef6.
4. Estonia's submission of the country report for this FUR preceded a Plenary decision to amend the Rules of Procedure for the 5th Round of Mutual Evaluations. Therefore, the 2013 version of the Methodology applies to this technical compliance re-rating exercise.
5. Available at Market in Crypto-Assets Act–Riigi Teataja.
6. Available at Money Laundering and Terrorist Financing Prevention Act–Riigi Teataja.
7. By way of comparison, there were 369 valid VASP licenses in 2022 (see the 2022 MER, paragraph 588).

services up to obtaining a CASP licence or until 30th of July 2026, upon which their licences become invalid. Up to that point they remain under the AML/CFT supervision of the EFIU.

Estonia has continued its national ML/TF risk assessment covering years 2021 - 2024. The results are planned to be adopted by the anti-money laundering and combating the financing of terrorism Governmental Committee by the end of September 2025.

III. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

9. This section summarises the progress made by Estonia to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER and applicable subsequent FUR for which the authorities have requested a re-rating (Recommendation (R.) 7 and R.15).

10. For the rest of the Recommendations rated as partially compliant (PC) (R.1, R.8, R.13, R.19, R.20, R.21, R.23, R.24, R.25, R.28, R.33, R.35) the authorities did not request a re-rating.

11. 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 Estonia submitted its country reporting template – at least six months before the FUR is due to be considered by MONEYVAL.[8]

IV. PROGRESS TO ADDRESS TECHNICAL COMPLIANCE DEFICIENCIES IDENTIFIED IN THE MER AND SUBSEQUENT FURS

12. Estonia has made progress to address the technical compliance deficiencies identified in the 2022 MER and the 2024 FUR. As a result of this progress, Estonia has been re-rated on R. 7 and R.15.

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

V. CONCLUSION

14. Overall, in light of the progress made by Estonia since its 1st Enhanced FUR was adopted, its technical compliance with the Financial Action Task Force (FATF) Recommendations has been re-rated as follows.

8. 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 of the plenary. 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.

Table 1. Technical compliance with re-ratings, September 2025

R.1	R.2	R.3	R.4	R.5
PC (MER)	C (MER)	LC (MER)	C (MER)	LC (MER)
R.6	R.7	R.8	R.9	R.10
LC (FUR1 2024) ~~PC~~	**LC (FUR2 2025)** ~~PC (FUR1 2024) PC~~	PC (MER)	C (MER)	LC (MER)
R.11	R.12	R.13	R.14	R.15
C (MER)	LC (MER)	PC (MER)	LC (MER)	**LC (FUR2 2025)** ~~PC (FUR1 2024) PC~~
R.16	R.17	R.18	R.19	R.20
C (MER)	LC (MER)	LC (MER)	PC (MER)	PC (MER)
R.21	R.22	R.23	R.24	R.25
PC (MER)	LC (MER)	PC (MER)	PC (MER)	PC (MER)
R.26	R.27	R.28	R.29	R.30
LC (MER)	LC (MER)	PC (MER)	LC (MER)	C (MER)
R.31	R.32	R.33	R.34	R.35
C (MER)	LC (MER)	PC (MER)	LC (MER)	PC (MER)
R.36	R.37	R.38	R.39	R.40
LC (MER)	LC (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).

15. Estonia will remain in enhanced follow-up and will continue to report back to MONEYVAL on progress to strengthen its implementation of anti-money laundering and combating financing of terrorism (AML/CFT) measures. In line with Rule 23 of the Rules of Procedures for the 5th Round of Mutual Evaluations, Estonia is expected to report back in one year's time.

Annex A: Reassessed Recommendations

Recommendation 7 – Targeted financial sanctions related to proliferation

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, maintained at PC)
FUR2	2025	↑ LC (upgrade requested)

1. In the 5th round MER of 2022, Estonia was rated PC. Identified shortcomings included: (i) the requirement to freeze assets is applied in limited circumstances only; (ii) the scope of assets that should be considered when implementing freezing obligations is limited; (iii) no provisions protecting the rights of bona fide third parties; and (iv) gaps in sanctions provisions for failure to comply. In its 2024 FUR, Estonia did not address all identified deficiencies and R.7 remained rated as PC. The following deficiencies remained: (i) the requirement to freeze assets did not apply in all circumstances; (ii) limited scope of assets subject to freezing obligation; (iii) the prohibition to make funds and other assets available applied only to designated persons and listed activities; (iv) the mechanisms for reconsideration of designations do not explicitly provide the competent authority or the process; (v) limitations of the sanctions set forth for the failure to comply with obligations under R.7; (vi) no provisions permitting additions to accounts or payments due under contracts, agreements or obligations that arose before the property became subject to freezing. Estonia implements PF TFS through EU decisions and regulations, complemented by domestic legislation.[9]

2. **Criterion 7.1** – *At the EU level*, implementation of TFS, pursuant to UNSCR 1718, does not occur "without delay." This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages.

3. *At the national level*, Estonia implements the UN TFS "without delay". International sanctions imposed by a UNSCR are implemented under the conditions laid down in the resolution with regard to the subjects of the international sanctions listed by the Committee established on the basis of the resolution until the regulation of the Council of the European Union is updated or adopted (ISA, §8). Thus, the UNSCRs are enforced in Estonia as of the day of adoption, before transposed into the EU legislative framework.

4. **Criterion 7.2** – In Estonia, the MFA is a co-ordinating body for implementation of the international sanctions (ISA, §10(1)). The EFIU is a designated authority for the implementation and enforcement of the TFS under the Estonian national legislation (ISA, §11(3)3)). The EFSA exercises supervision over compliance with the application of financial sanctions by its supervised OEs (ISA, §30(1.1)). The Bar Association and the Ministry of Justice (or when delegated - the Chamber of Notaries) carry out supervision of lawyers and notaries (ISA, §30(4), (5)).

(a) At the EU level, all natural and legal persons within the EU are required to freeze the funds or other assets of designated persons or entities as soon as a designation is published, i.e. without prior notice (EU Regulation 2017/1509, art.1and 2). Though delays in implementation apply as described under c.7.1.

At the national level, the regulatory framework and the identified deficiencies as described under c.6.5(a) apply.

9. At the EU level, UNSCR 1718 (2006) on DPRK and its successor resolutions are implemented through Council Decision 2016/849/CFSP and EU Regulation 2017/1509.

(b) At the *EU level*, freezing actions for UNSCR 1718 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, and includes assets generated from such funds. (EU Regulation 2017/1509, art. 1 and 34).

This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35).

While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds 'controlled' by the designated person (Para 55b. of the Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy).

At the national level, the obligation to freeze extends to funds and economic resources of a designated person or entity (ISA, §5, §14(1), §19 and §21(1)), including when those are owned jointly (§15(1)), as well as to funds and economic resources of a person or entity *related* to a designated person in the cases and under the conditions specified in the legislation imposing or implementing international sanctions (ISA, §14(2)). Although not explicitly defined in law, the concept of a person or entity *related to* the subject of a sanction is outlined in the explanatory memorandum of the act amending the ISA in May 2024. The specific criteria for determining that a person or entity is owned, held or controlled by a subject of the sanction, or act under its instruction, are considered to be those established by the instrument imposing an international sanction. The explanatory memorandum further clarifies that, in most cases, this includes persons or entities who are directly or indirectly, wholly or partly, owned, held or controlled by the subject of the sanction, or who act under its instructions. This interpretation is confirmed by the EFIU guidance on sanctions of 30 May 2025, which also covers explicitly the persons who act on behalf a designated person or entity, a criterion not addressed in the explanatory memorandum (EFIU Guidance on sanctions, §3.1.1).

(c) At the *EU level*, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU regulation 2017/1509, art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU.

At the national level, the ISA covers both freezing of funds and economic resources and preventing financial and economic resources being made available to designated persons and entities (ISA, §14(1)(2)). This extends to person and entities *related to* the subjects of financial sanctions, as described under sub-criterion 7.2(b).

(d) At the EU level, the same mechanism to communicate PF TFS is used as for TF TFS (see c.6.5(d)).

At the national level, the MFA is responsible for informing the public immediately regarding the imposition or amendments regarding designated persons and entities through its website and other information channels (ISA, §10(1)(4))). In 2025, the EFIU issued two revised guidelines on sanctions – one applicable to all natural and legal persons, and another one specifically addressed to reporting entities. The EFSA 2021 guidelines on sanctions apply to banks and other supervised financial institutions.

(e) At the *EU level*, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations. (EU Regulation 2017/1509, art. 50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations.

At the national level, the regulatory framework as described under c.6.5(e) applies.

(f) At the *EU level*, protections are in place for third parties acting in good faith (EU Regulation 2017/1509, art.54).

At the national level, there are provisions to protect the rights of *bona fide* third parties acting in good faith when implementing international financial sanctions (ISA, §6[1]).

5. **Criterion 7.3** – *At the EU level,* member states are required to take all necessary measures to ensure that the EU Regulations on this matter are implemented and to determine a system of effective, proportionate, and dissuasive sanctions in line with EU Regulations (EC Regulation 2017/1509, Art.55(1) and EC Regulation 267/2012, Art.47(1).

6. *At the national level,* the EFIU is a designated authority for the state supervision over the application of financial sanctions and compliance with requirements of the ISA and a legislation established on the basis of thereof by persons with special obligations (ISA, §30(1)). At the same time, the EFSA exercises supervision over compliance of application of financial sanctions by its supervised OEs (ISA, §30(1.1)). The TFS supervision of lawyers and notaries is carried out by the Bar Association and the Ministry of Justice (or when delegated - the Chamber of Notaries) (ISA, §30(4),(5)). Other DNFBPs are subject to state supervision carried out by the EFIU over the application of TFS by natural and legal persons (ISA, §20(1), §30(1)). The LEAs may also exercise state supervision over implementation of the ISA (ISA, §31).

7. Estonia has a wide range of sanctions for non-compliance with the obligations under R.7, including criminal sanctions for both intentional and negligent violations, as well as extended confiscation measures of assets acquired through intentional breaches. All available sanctions are generally considered proportionate, with the exception of those imposed under the misdemeanour proceedings, which raise certain concerns regarding their comprehensiveness and proportionality (see point (b) hereunder). Nevertheless, these concerns are assessed as minor given the overall range of available sanctions. A detailed description of the applicable sanctions is provided below.

(a) Under the administrative proceedings the EFIU and EFSA may issue a precept to suspend the transaction, or acts suspected of violation or oblige taking measures necessary for the application of the non-compliance levy (ISA, §32; FSAA, §18(2)4), §55(1)). There are proportionate sanctions set for non-compliance with the percept set for the covered FIs and other natural and legal persons (thus covering non-covered FIs and all DNFBPs) (ISA, §33).

(b) Under the misdemeanour proceedings the sanctions set extend to the violation of a requirement to notify the EFIU of identification of a listed person or entity, or violation of financial sanctions, or submission of false information (ISA, §35). However, those cover only persons with special obligations which include only the covered FIs and DNFBPs and do not extend to the violation of an obligation of freeze without delay and without prior notice. Violation of a notification requirement, violation of financial sanctions or filing false information is punishable by a fine of up to 300 fine units (1 200 euros (EUR)) or by detention and the same act, if committed by a legal person - is punishable by a fine of up to EUR 400 000. The limitations of the misdemeanour proceedings as described under c.35.1 may impact the proportionality of these sanctions.

(c) Under the disciplinary proceedings the Bar Association, the Ministry of Justice and the Chamber of Notaries may apply sanctions to the lawyers and notaries. The range of available sanctions for the limited scope of obligations as per ISA (§24), including the maximum amount of fine which can be imposed, appears to be proportionate (see also c.35.1).

(d) In addition, there is a criminal liability set for the failure to comply with obligations provided by legislation implementing international sanctions or for violation of the prohibitions, including

through negligence (PC, §93.1; §93.3). Sanctions are set for both natural and legal persons. Pecuniary punishment or up to five years' imprisonment are set for the natural person and the same act, if committed by a legal person, is punishable by a pecuniary punishment. The court may impose extended confiscation of assets acquired by the criminal offence under §93.1 of the PC.

8. **Criterion 7.4** –

(a) At the *EU level*, listed persons are informed of their ability to petition the UN Focal Point or their own government for de-listing, through the EU Best Practices document for the effective implementation of restrictive measures (page 11, para. 23).

At the national level, on the MFA website the public is provided with a link to the UN Focal Point for de-listing to inform about the mechanism for applying to the UN directly.

(b) At the *EU level*, procedures for unfreezing funds due to cases of mistaken identity are the same as those described under c.6.6(f).

At the national level, procedures described under c.6.6(f) are applicable.

(c) At the *EU level*, the regulation imposing TFS obligations under UNSCR 1718 contains measures for national competent authorities to authorise access to frozen funds or other assets under the conditions set out in UNSCR 1718. (EU Regulation 2017/1509, art. 35-36).

At the national level, the regulatory framework as described under c.6.7 applies.

(d) At the *EU level*, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c7.2(d) also contains information on the obligations to respect a de-listing action.

At the national level, the MFA is responsible for informing the public immediately regarding the imposition or amendments regarding designated persons and entities through its website and other information channels (ISA, §10(1)(4))). In 2025, the EFIU issued two revised guidelines on sanctions – one applicable to all natural and legal persons, and another one specifically addressed to reporting entities. The EFSA 2021 guidelines on sanctions apply to banks and other supervised financial institutions.

9. **Criterion 7.5** – With regard to contracts, agreements or obligations that arose prior to the date on which the account became subject to TFS:

(a) At the *EU level*, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EU Regulation 2017/1509, art. 34(9)).

At the national level, Estonia implements UNSC resolutions directly before EU adopts them. All obligations, including permitting the addition to the accounts or payments due under contracts, agreements or obligations that arose prior to the date on which the property became subject to freezing are implemented directly through UNSC resolutions.

(b) This sub-criterion is not applicable, as the TFS elements of UNSCR 2231 expired on 18 October 2023. Therefore, this analysis did not assess the implementation of UNSCR 2231.

Weighting and Conclusion

10. Estonia implements the UNSCRs on PF in a timely manner. All the requirements set out under R. 7 are met or mostly met. Minor shortcomings remain with respect to the limited circumstances in which the requirement for freezing assets applies, and the comprehensiveness and proportionality of the misdemeanour sanctions. **R.7 is re-rated to LC.**

Recommendation 15 – New technologies

	Year	Rating and subsequent re-rating
MER	2022	PC
FUR1	2024	PC (upgrade requested, maintained at PC)
FUR2	2025	↑ LC (upgrade requested)

1. In the 5th round MER of 2022, Estonia was rated PC with R.15. Identified shortcomings included: (i) new technology risk assessments are not always accompanied with in-depth analysis; (ii) no explicit requirement to undertake risk assessment prior to the launch or use of new products, practices and technologies; (iii) no specifically designated authority for detecting unlicensed VASP activities; (iv) need for further guidance of sector specific typologies, in particular on TF; (v) the impact of the shortcomings identified under c.35.1 and c. 7.3 related to the sanctioning regime; (vi) deficiencies related to VA transfers; (vi) no guidance for VASPs on the freezing and reporting obligations. In its 2024 FUR, Estonia did not address most of the deficiencies identified by the MER of 2022 and R.15 remained rated as PC.

2. **Criterion 15.1** – At the national level, in 2016 Estonia conducted an analysis of ML/TF risks related to the remote identification of customers; in 2021 the NRA analysed the ML/TF risks related to the use of VAs, FinTech (crowdfunding and VASPs); in 2021 sectoral risk analysis identified the risks related to provision of payment services within the framework of correspondent relationship to customers who are FIs providing VA services; in 2022 the sectoral risk assessment looked into the ML/TF risks posed by the VA transactions. These were followed by a more in-depth analysis of the risks related to VASPs/VAs by the EFIU in 2024. The VASP sectorial risk matrix is regularly updated based on quarterly reports submitted by VASPs, as well as off-site questionnaires issued by the EFIU on a as-needed basis (the most recent issued in 2023). Estonia has also carried out its national risk assessment for the period 2021-2024, which updates the risks associated with new technologies, with a particular focus on the use of artificial intelligence and the threats posed by deepfake technology. However, the results this assessment are planned to be adopted by the end of September 2025.

3. With regard to covered FIs, they are required to identify and assess the risks of ML/TF related to new and existing products, services, including new or non-traditional delivery channels and new or emerging technologies (MLTFPA, §13(1)3)4) and §14(1)6)).

4. **Criterion 15.2** –

(a) The covered FIs are required to undertake the risk assessment of products, practices and technologies, including the new and emerging ones, which should be updated where necessary, and on the basis of the NRA (MLTFPA, §13(1)3)4), §13(4)). While there is no explicit requirement to undertake a risk assessment *prior to* the launch or use of such products, practices and technologies, the revised EBA Guidelines on ML/TF risk factors[10] (EBA/2021/02), implemented by the EFSA in August 2024, clarifies that the ML/TF risk exposure shall be assessed prior to the launch of these products, services or business practices (p.1.7(d)).

The EFSA Advisory AML/CFT Guideline recommends that the risk assessment must also be reviewed if the obliged entity decides to change the services provided and products offered, or use new or updated sales channels, which might suggest a prior risk assessment.

(b) The covered FIs shall have procedures that provide effective mitigation and management of risks relating to ML/TF and ensure the adherence with those (MLTFPA, §14(1)(2)).

10. Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849.

5. **Criterion 15.3** –

(a) At EU level, the European Commission conducts and publishes an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Art. 6) that also identifies and assesses the risks emerging from virtual assets and the activities and operations from VASPs. The EU level risk assessment shall be updated by a report at least every two years.

In Estonia, the ML/TF risks related to the VA activities and VASPs were assessed within the scope of the NRA of 2021, the sectorial risk assessment of the EFSA from 2021, and the EFIU – from 2020 and 2022.

The NRA of 2021 identified that the VASP sector is exposed to high ML and TF risks. The main ML risks in the sector are related to VASPs with activity licenses issued in Estonia that are used for committing (investment) frauds abroad, for converting proceeds of fraud into virtual currencies, for conducting exchange operations through ATMs using cash thus impeding an appropriate identification of a customer, and transactions with non-resident customers from high-risk jurisdictions. As concerns the TF risks related to the VASP sector, those were the use of VASPs by the sanctioned persons or by persons with extreme Islamic views and by non-resident customers from high-risk jurisdictions. With respect to the vulnerabilities in the VASP sector, those were identified to be similar for the purposes of ML and TF: (i) the insufficient legislative framework (including the coverage of the VASPs) and resources for ensuring an appropriate level of entry requirement checks and supervision of the rapidly growing VASP market, with a weak link to Estonia (until 2020); (ii) poor application of preventative measures (including weaknesses in identification and verification of customers and compliance control systems) and reporting by the VASP sector. The NRA of 2021 acknowledged that the available quantitative and qualitative data did not allow for the establishment of patterns, the profile of criminals or suspicious activities related to VASPs in Estonia (see also c.1.1). Since then, access to quantitative and qualitative data has expanded through the introduction of mandatory reporting requirements for credit institutions and VASPs (since September 2023). The EFIU also conducted an analysis of the Estonian VASP wallet addresses in 2024. Together with information from the STRs, this enabled the identification of main patterns, including high transaction volumes by legal persons, the involvement of legal entities resident in offshore jurisdictions, and the most common ML threats in VASP sector, such as fraud, identity theft, forged documents and dark web related activities. The outcomes of this analysis are included into the VASP risk matrix and supported the update of the ongoing national risk assessment, which is expected to be adopted by the end of September 2025.

The EFSA SRA from 2021, identified the risks related to the provision of payment services within the framework of correspondent relationships to customers who are FIs providing VA services.

The EFIU Survey of VASPs from 2020 analysed the schemes and practices of unlawful use of the VAs. The findings of this analysis were further incorporated into the NRA 2021. Further on, in 2022 the EFIU conducted the second analysis of the VASP market. In this study more diversified sources of information were used, such as the LEA information and foreign co-operation requests including the MLAs (Mutual Legal Assistance). The study highlighted fraud, ransom, and drug crime as the prevailing threats. As per the vulnerabilities, those in the majority of instances reiterated the findings of the NRA highlighting the weak connection of the licensed VASPs with Estonia, including the seat addresses (use of identical address by approx. 2/3 of VASPs or

unknown addresses),[11] nominal board member and shareholder (nearly 75% have a CSP among associated persons),[12] a small number of local employees (15 largest VASPs had a total of 27 employees in Estonia).[13]

To enhance the VASP sectorial risk matrix, EFIU uses data from VASP periodic reporting and off-site questionnaires. The EFIU data team is tasked with refining the risk matrix from a technical perspective. EFIU has devised a methodology, and the data team is utilising the information from VASP periodic reports to automate updates to the sectorial risk matrix. While the results of those analyses were used to prepare in-house summaries, issue several thematic reports, and enhance risk-based supervision, there was no publication of an updated NRA or sectoral risk assessment.

(b) Following the adoption of the NRA of 2021 Estonia developed and adopted on 5 July 2021 an Action Plan for implementation of AML/CFT measures for the period of 2021-2024. Those respective actions are prioritised in line with the level of the identified risks. The actions for mitigation of risks identified in the VASP sector as a high ML/TF risk sector are given a high priority. With this purpose Estonia had revised the MLTFPA by 15 March 2022, strengthening the requirements for the licensing regime and for the application of preventatives measures (including identification and verification of customers and compliance control systems). The mitigation actions for the risks identified in the updated risk assessment exercise remain to be clarified.

Since the mutual evaluation, Estonia has passed a regulation establishing mandatory reporting requirements for credit institutions and virtual asset service providers, which came into effect on 18th of September 2023; this should contribute to more efficient supervision and strategic analysis capability in the sector of VASPs.[14]

(c) VASPs are required to take appropriate steps to identify, assess, manage and mitigate their ML/TF risks as set out in c.1.10 and 1.11 (MLTFPA, §§13,14).

6. **Criterion 15.4** –

(a) A person providing crypto[15] asset services within the EU is subject to prior authorisation (EU Regulation 1114/2023, Art. 59) by the authority of the member state where it has its registered office. A crypto asset service provider under EU law should be a legal person or other undertaking if the legal form of that undertaking ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if it is subject to equivalent prudential supervision appropriate to their legal form (Art. 59 (3)). These requirements to the legal form of undertakings exclude natural persons from being authorised as crypto asset service providers (c.15.4 (a) (ii) is not applicable).

EU law also subjects some types of offerors to authorisation requirements and differentiates offerors according to the specific assets: A person that issues virtual assets qualifying as asset-referenced tokens (EU terminology for a type of stable-coins) has to be authorised as well (EU Regulation 2023/1114, Art. 16). E-money tokens may only be issued by authorised credit institutions or e-money institutions (EU Regulation 2023/1114, Art. 48). Financial services related to an issuer's offer and/or sale of a virtual asset are covered in the crypto-assets services

11. The SRA related to VASP sector, p.5 and 19.
12. The SRA related to VASP sector, p.19.
13. The SRA related to VASP sector, p.20.
14. In addition, Estonia has published Typology Message 9TT202408. However, this was not published until 8 August 2024 and therefore after the cut-off date for information to be taken into account for this FUR.
15. In the terminology of the EU Regulation 1114/2023 on markets in crypto-assets 'virtual asset' and 'virtual asset service provider' as per the FATF Glossary are defined as 'crypto asset' and 'crypto asset service providers' respectively. Here, both terms are used depending on the framework referred to.

list under Art. 3 (1)(16) EU Regulation 2023/1114, in line with the provisions of the FATF glossary and the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[16] for limb (v) of the VASP definition in the FATF glossary.

Authorisation processes for service providers and offerors include a fit and proper assessment and authorisations shall only be granted if members of the management bodies and shareholders or members are of sufficiently good repute (Art. 21 (2), 63 (10) EU Regulation 2023/1114).

Since the last follow-up report, Estonia has adopted the Market in Crypto-Assets Act (MCAA), implementing EU Regulation 1114/2023, which entered into force on 1 July 2024. Along with the MCAA, the MLTFPA was amended, with the new provisions taking effect on 30 December 2024.

The definition of VASPs in the MLTFPA covers all five activities as defined by the FATF (MLTFPA, §3(9[1])-(10[3]). The MLFTPA § 6 section 2 subsection 3[1] defines crypto-asset service provider, within the meaning of point 15 of paragraph 1 of Art. 3 of the EU Regulation 2023/1114, as a financial institution for the purpose of application of the MLTFPA.

In order to operate, participants in crypto-asset markets are required to obtain an authorisation from the EFSA, which has also been designated as the competent authority within the meaning of the EU Regulation 2023/1114 to supervise crypto-asset market participants (MCAA, §5, §26).

VASPs which had the right to provide virtual currency services on the basis of the MLTFPA before 30 December 2024, must bring their activities into compliance with the requirements provided by the MCAA and apply for an authorisation to the EFSA no later than by 1 July 2026.

(b) Authorisation processes under EU Regulation 2023/1114 include assessments that members of the management body are sufficiently reputable and competent and that shareholders or members that have a qualifying holding fulfil fit and proper requirements (Art. 62, 63, 64 and 68 for crypto asset service providers). These provisions empower authorities to prevent individuals convicted of offences relating to money laundering or terrorist financing or of any other offences that affect their good repute from assuming relevant functions. Regarding shareholders and members whether direct or indirect, that have qualifying holdings, proof is required that those persons are of sufficiently good repute (Art. 62 (2) (h)).

An application for an authorisation to provide crypto-asset service submitted to the EFSA must comply with the requirements of Art. 60, 62, 68 of the EU Regulation 2023/1114 (MCAA, §6(1), §7(2), §48(8)).

7. **Criterion 15.5** – Regulation at EU level prohibits the provision of services without authorisation (Art. 59 (1) EU Regulation 2023/1114). EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure action is taken to identify persons that carry out VASP activities without licensing or registration and to ensure compliance with authorisation requirements by taking supervisory measures and applying sanctions. EU Regulation 2023/1114, Art. 94 (1) (h) stipulates that competent authorities, in accordance with national law, shall have the power to order the immediate cessation of the activity where there is a reason to assume that a person is providing crypto-asset services without authorisation. The prerequisite of "reason to assume" the provision of service leaves sufficient room to take targeted action at service providers that address the market.

16. Available at www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.

8. At EU level, the European Securities and Markets Authority assist efforts to ensure compliance by keeping a register of operators found to have provided services in breach of the authorisation requirement (Art. 110 EU Regulation 2023/1114).

9. Estonia has designated the Police and Border Guard Board to be the default authority for detecting breaches of licensing provisions (the Police and Border Guard Act). In the circumstances when the unlicensed VASP activity is carried out by an entity that is licensed for providing services falling within the covered FIs or covered DNFBPs without prior notification of change of a business model, or in breach of restriction related to office (for notaries), or legal restrictions imposed on activities of advocates (for lawyers) the respective licensing or authorising authority, i.e., EFSA, EFIU, Bar Association or Chamber of Notaries are those responsible for detection and sanction (FSAA, §6(1)41) and 18(2)1), MLTFPA, §§74, 75, 97; BAA, §19, §821; NA, §12, §17(2)). The respective sanctioning powers can be imposed in those circumstances (see R.35).

10. In order to detect unlicensed VA activities, the EFIU uses the following main sources of information: the STR or other reports filed by the OEs, information received from the foreign counterparts, and the PGDB database. The EFIU routinely searches social media and other public advertisements for businesses which operate in the regulated sector and are not appropriately licensed.

11. In the circumstances when the unlicensed VASP activity is carried out by the undertaking that is not a covered FI or covered DNFBP a criminal report should be filed to the investigative authority or the Prosecutor's Office (CCP, §195(1)). Economic activities without an activity licence are a criminal offence pursuant to PC, §372 (see c.35.1).

12. According to information provided by the Estonian authorities, in the period 2022-20254, the EFIU disseminated four cases of detected unlicensed VASP activity to the LEAs. In one case, the license was withdrawn, one case was dismissed, and two other cases remain under investigation.

13. **Criterion 15.6** –

(a) When assessed for market entry, crypto asset service providers are required to have mechanisms and controls in place that ensure compliance with AML/CFT requirements (EU Regulation 2023/1114, Art. 63 (2) to (10)).

For VASPs operating under an authorisation granted pursuant to the MLTFPA, the EFIU is the designated supervisory authority for VASPs in ensuring compliance with the AML/CFT framework (until 1 July 2026) (MLTFPA, §64(1)). The EFSA acts as a supervisory authority in the circumstances when the VASP services are provided by a service provider that is operating on the basis of a license/authorisation issued by the EFSA (MLTFPA, §64(2), §70(2)). As of 30 December 2024, the EFSA is the designated supervisory authority for the crypto asset service providers operating under an authorisation granted under the MCAA (MCAA, §26). To date, no such authorisation has been issued. The EFIU and the EFSA are required to apply a RBA when supervising entities providing VA services (Code of Conduct for the Supervision Activities, §1.5; EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §5.1). The authorities clarified that the EFIU's internal rules of supervisory procedure require the VASP risk matrix to be supplemented with information gathered during on-site/off-site inspections, as well as with data obtained from the mandatory regular reports submitted by VASPs. These reports include information on high-risk customers, clients' country of residence and the implementation of EDD measures. The EFSA's RBA model considers internal procedures, identified deficiencies, and the proportionality of these deficiencies with the scope of the entity's business activities or the number of clients. The country also informed that a new RBA model is being developed by the EU Authority for anti-Money laundering and countering the financing of terrorism (AMLA)

working groups and will be implemented in the future. Both supervisory authorities should revise the assessment of ML/TF risk profile of VASPs annually or in case of emerging trends, major events or developments. In the case of the EFSA, this is required by the AML/CFT rules of procedure (EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §1.12, §3.3). For the EFIU, there is no such formal obligation. However, the authorities advised that the 2021 Risk Matrix tool is required to be updated regularly, at least once a year, and take into account new typologies and emerging risks in the supervised sectors. (see also c.26.6).

(b) EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure compliance by crypto asset service providers with requirements to combat money laundering and terrorist financing. EU Regulation 2023/1114, Art. 94, stipulates that competent authorities in accordance with national law shall have the power to inspect and to compel documents. The withdrawal of the authorisation of crypto asset service providers is regulated at EU level in Art. 64 of EU Regulation 2023/1114 and, alongside other administrative penalties and administrative measures, shall also be implemented at national level (EU Regulation 2023/1114, Art. 111).

Both supervisors, the EFIU and the EFSA (as applicable), have powers to supervise the VASPs and take appropriate measures to ensure compliance with AML/CFT requirements (MLTFPA, §54(1)4), §64(1) and (2); FSAA, §6(7); SFIU, §7(4)). Both supervisors have powers to conduct on-site and off-site inspections of VASPs, or a combination of both methods (MLTFPA, §66; AML Rules of Procedure of the EFSA, §2.6; Code of conduct for the supervision activities of the EFIU, §2.2). They are empowered to compel OEs to provide information without the need for a court order (MLTFPA, §58(1) and §66; FSAA, 22.1(1)1)) (see also the R.27). Both supervisory authorities are empowered to apply to VASPs a range of administrative and misdemeanour measures, including the revocation of a license fully or partially (see c.35.1).

14. **Criterion 15.7** – After amendment by EU Regulation 2023/1113 EU Directive 2015/849 (Art. 18) mandates the European Banking Authority to issue guidelines on risk variables and risk factors to be taken into account by crypto-asset service providers when entering into business relationships or carrying out transactions in crypto-assets. (Guidelines published on 16 January 2024 and to be applied from issued from 30 December 2024).

15. There are no VASP-specific guidelines established in Estonia. Nevertheless, the EFIU issued three guidelines that reflect on the characteristics of reports; the reporting obligation, the management of risks relating to ML/TF and the application of due diligence issued in 2019 and 2022 respectively. In addition, the EFIU has been providing the VASPs with sector-specific feedback since 2020, and in 2023 the EFIU published an overview of sanctions evasion through the use of virtual currencies. The EFIU also published a short survey regarding financing models of a terrorist organisation, which includes virtual currency-related risk indicators, as well as an example case demonstrating how VASPs can be utilised. The EFIU has engaged with the VASP sector through a TF initiative launched in 2023, which continued into 2024 and has since evolved into a recurring annual or bi-annual exercise. Complementing this, the EFIU delivered sector-specific training throughout 2024–2025 (6 trainings), including on TF typologies, and provided further guidance through high-level materials and case studies published in the EFIU Yearbook.

16. **Criterion 15.8** –

(a) EU Directive 2015/849 and EU Regulation 2023/1114 require member states to provide competent authorities, in accordance with national law, with the power to apply appropriate administrative penalties and other administrative measures. Art. 111 of EU Regulation 2023/1114 stipulates sanctions for a number of infringements including minimum fines.

Most financial sanctions are proportionate. Sanctions covered by §§ 94^2, 95, and 96^1 of the MLTFPA are not considered proportionate.

The limitation period for misdemeanour proceedings is not considered enough for failure to submit beneficial owner information or submission of false data. The concerns regarding the limitations of the misdemeanour procedure described under c.35.1 remain.

Additional sanctions were introduced in the MLTFPA (§96^2) for breaches of the obligations related to the transfer of crypto-assets, implementing the requirement of the EU Regulation No. 2023/1113 on information accompanying transfers of funds and certain crypto-assets (EU Regulation 2023/1113), which are assessed as proportionate.[17]

Regarding administrative measures for imposing non-compliance levies, while the maximum limits that can be imposed by the EFSA on PSPs and EMIs, including those carrying out VA related activities, have been increased (in force since 01.11.2023), the limits applicable to VASPs by the EFIU remain unchanged and were considered insufficiently proportionate in the 2022 MER (see c.35.1).

(b) At EU level, member states are obliged to ensure that where obligations apply to legal persons in the event of a breach, sanctions and measures can be applied to the members of the management body and to other natural persons responsible for the breach (Art. 58 (3) of EU Directive 2015/849). Some of the administrative penalties regulated under EU Regulation 2023/1114, Art. 111, shall also apply to members of the management body of a crypto-asset service provider.

The administrative measures i.e., precepts, are issued to legal persons. Nevertheless, depending on their scope, they can have a direct impact or effect on the natural persons, including the directors and senior management of the VASP (e.g., when the precept demands the removal of a manager of a VASP, or the temporary suspension of his/her authority). The financial penalties pursuant to the misdemeanour proceedings may be imposed on both natural and legal persons, thus being applicable to the directors and senior management of the VASPs. (see c.35.2).

17. **Criterion 15.9** – With respect to the preventive measures, VASPs are required to comply with the requirements of R.10-21 in the same manner as the covered FIs and are subject to the same deficiencies. The application of the preventive measures by VASPs is subject to the following qualifications.

(a) The VASPs are not allowed to provide services outside a business relationship (MLTFPA, §25(1^3). The requirement to conduct CDD (customer due diligence) applies to all transactions regardless of any threshold.

(b) (i) EU Regulation 2023/1113 repeals and replaces EU Regulation 2015/847 formerly regulating the transfer of funds and extends the scope to cover both transfer of funds and transfer of virtual assets. Art. 14 (1) of EU Regulation 2023/1113 requires the originating crypto asset service provider to obtain and hold originator information (Art. 14 (1), (2) and (3)) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Art. 14 (4)). Before transferring crypto-assets, the service provider shall verify the accuracy (Art. 14 (6). In accordance with Art. 24 of EU Regulation 2023/1113, information has to be provided to competent authorities in the Member State in which they are established. The originating crypto asset service provider submits beneficiary information to the beneficiary's service provider in

17. For natural persons - a fine of up to EUR 5 mil. or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented and for legal persons – in addition to the pecuniary penalty provided for natural persons, up to 10% of the consolidated turnover of the legal person or of the person's consolidation group (§962 of the MLTFPA).

line with Art. 14 (2) of Regulation 2023/1113 and holds it on record according to Art. 26 (1) Regulation 2023/1113.

The distributed ledger address (DLT) information is required for both the originator and the beneficiary. If the transfer does not occur on the DLT, the Regulation requires the crypto-asset account number instead (EU Regulation 2023/1113, Art.14 (1) (b) and (2) (b)).

EU Regulation 2023/1113 imposes additional requirements to be implemented in the case of transfers being made to self-hosted addresses (where no crypto asset service provider is involved on the originator or beneficiary side), such as individual identification of transfers and ensuring that the address is controlled by the originator/beneficiary.

EU Regulation 2023/1113 does not make a distinction between crypto-asset transfers within and outside the EU, treating all crypto-asset transfers as cross-border.

(ii) Art. 16 of EU Regulation 2023/1113 requires the crypto asset service provider of the beneficiary to implement effective procedures, which may include post-event or real-time monitoring, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (EU Regulation 2023/1113, Art. 16 (1) and (3)). Service providers are obliged to make information available to competent authorities on request according to Art. 24 of EU Regulation 2023/1113.

(iii) EU Regulation 2023/1113 covers the requirements of Recommendation 16 and applies them to virtual asset transfers, especially on monitoring and risk-based procedures (Art. 14 (8) and Art. 16 (1)) as well as freezing action and prohibiting transactions with designated persons and entities (Art. 23).

(iv) Financial institutions are covered by the scope of relevant provision of EU Regulation 2023/1113 through the broad definition of crypto asset service provider in Art. 3 (1) 15 of that Regulation with reference to Art. 3 (1) (15) EU Regulation 2023/1114, including credit institutions that provide crypto asset services in accordance with Art. 59, 60 of EU Regulation 2023/1114.

18. **Criterion 15.10** – The communication mechanism and the TF/PF TFS obligations apply to VASPs in the same manner as they apply to other reporting entities. Please refer to analysis of criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) as they apply to VASPs.

19. Since the last follow-up report, the EFIU has issued revised guidelines (May 2025) on the obligations of the reporting entities, including VASPs, under the ISA. The EFSA has implemented (May 2025) the EBA Guidelines on internal policies, procedures and controls to ensure the implementation of the Union and national restrictive measures under EU Regulation 2023/1113. The guidelines address both payment and crypto-asset service providers and provides specific guidance on freezing and reporting obligations (§4.3).

20. In 2024, the EFIU carried out outreach activities by distributing to all licensed VASPs a list of sanctioned or TF-linked cryptocurrency addresses and instructing them to report their findings based on screening these addresses. Further guidance was provided by the EFIU in 2024 by distributing to VASPs a typology report outlining the risks posed by certain platforms for sanctions evasion or money laundering.

21. Following the amendments to the ISA of June 2024 (which entered into force in January 2025), VASPs, alongside other reporting entities, are required to report to the EFIU, not more frequently than once a month, on the measures implemented under the ISA, providing information on persons, funds, economic resources, accounts, payments, transactions and other relevant data (ISA, §32[1]).

22. **Criterion 15.11** – EU Regulation 2023/1114, Art. 107, expressly provides that competent authorities should, where necessary, conclude co-operation arrangements with supervisory authorities of third countries concerning the exchange of information with those supervisory authorities of third countries and the enforcement of obligations under this Regulation in those third countries.

23. The international co-operation measures described in R.37 to R.40 apply to activities related to VAs or concerning VASPs. The deficiency with respect to issues on double-criminality requirement applies (see c.37.6). Both supervisory authorities have a right to exchange information and co-operate with their counterpart authorities of other countries based on the duties provided by the MLTFPA (§64(6)). Following the amendments of the Financial Supervisory Act introduced in July 2024, the international co-operation framework established for the EFSA (see c.40.12) equally applies to VA and VASPs. In addition, the EFIU is empowered to engage with the foreign FIU or a LEA with the purpose of ensuring implementation of the TFS by VASPs (ISA, §34)4-5)).

Weighting and Conclusion

24. Estonia requires the risk assessment of new technology and services when launching the products. It has a regulatory framework for VASPs and has conducted an ML/TF risk assessment of the VASPs sector in 2021 and 2022, with the process continuing in 2024-2025. Access to quantitative and qualitive data relevant to risk assessment has improved due to mandatory periodic reports from the sector. VASPs are required to be licensed and, as of March 2022, all five activities described by the FATF standard are encompassed by the definition of VASPs. In July 2024, the new legal framework on the markets in crypto assets entered into force (with the exception of certain provisions), implementing the EU requirements for the crypto asset markets. The introduction of EU level measures has addressed the shortcomings related to VA transfers. During 2023-2025, the sector was provided with guidance and training, including on TF typologies. Most of the requirements related to targeted financial sanctions have been implemented, with only minor shortcomings remaining. However, some deficiencies remain: (i) the results of the updated national risk assessment, which include risks associated with new technologies, have not yet been adopted; (ii) the mitigation actions for the risks identified in the updated national risk assessment exercise remain to be clarified; (iii) although subject to a broad range of sanctions, certain sanctions under the misdemeanour procedure and those impose by the EFIU for non-compliance with a percept are not sufficiently proportionate. **R. 15 is re-rated LC.**

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

Recommendations	Rating	Factor(s) underlying the rating[18]
7. Targeted financial sanctions related to proliferation	PC (MER 2022) PC (FUR1 2024) **LC (FUR2 2025)**	• Requirement to freeze assets is to be applied in the certain circumstances only, which limits the compliant application of those. (c.7.2(a)) • There are minor deficiencies regarding the misdemeanour sanctions-(c.7.3)
15. New Technologies	PC (MER 2022) PC (FUR1 2024) **LC (FUR2 2025)**	• The results of the national risk assessment, which include risks associated with new technologies, have not yet been adopted. (15.1) • The mitigation actions for the risks identified in the updated risk assessment exercise remain to be clarified. (15.3(b)) • Sanctions covered by 942, 95, and 961 and the maximum non-compliance levies that the EFIU can impose are not considered as proportionate. (15.8(a)) • The limitation period for misdemeanour proceedings is not considered enough for failure to submit beneficial owner information or submission of false data. (15.8(a)). • The minor shortcomings in relation to R.6 and R.7 apply. (15.10) • The deficiency with respect to issues on double-criminality requirement apply (see c.37.6). (15.11)

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

GLOSSARY OF ACRONYMS

AML/CFT	Anti-money laundering and combating financing of terrorism
C	Compliant
CASP	Crypto-asset service providers
DLT	Distributed ledger address
DNFBPs	Designated non-financial business or profession
EBA	European Banking Authority
EC	European Commission
EFIU	Estonian Financial Intelligence Unit
EFSA	Estonian Financial Supervision Authority
EMI	E-money institutions
EU	European Union
FATF	Financial Action Task Force
FI	Financial institution
FSAA	Financial Supervisory Authority Act
FUR	Follow-up report
ISA	International Sanctions Act
LC	Largely compliant
LEAs	Law enforcement agencies
MCAA	Market in Crypto Assets Act
MER	Mutual evaluation report
MFA	Ministry of Foreign Affairs
ML	Money laundering
MLTFPA	Money Laundering and Terrorist Financing Prevention Act
NC	Non-compliant
NRA	National risk assessment
OE	Obliged entity
PC	Partially compliant
PF	Proliferation financing
PSP	Payment Service Provider
R.	Recommendation
RBA	Risk-based approach
TC	Technical compliance
TF	Terrorism financing
TFS	Terrorism financing sanctions
UN	United Nations
UNSCR	United Nations Security Commission Resolution
VASPs	Virtual assets service provider
VA	Virtual assets

www.coe.int/MONEYVAL

September 2025

Follow-up report

Anti-money laundering and counter-terrorist financing measures -

Estonia

2nd Enhanced Follow-up Report &

Technical Compliance Re-Rating

This report analyses Estonia's progress in addressing the technical compliance deficiencies identified in the December 2022 assessment of their measures to combat money laundering and terrorist financing and in subsequent follow-up reports.