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(2022)11

Anti-money laundering and counter-terrorist financing measures

Estonia

Fifth Round Mutual Evaluation Report

December 2022

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 fifth mutual evaluation report on Estonia adopted by the MONEYVAL Committee at its 64th Plenary Session

(Strasbourg, 5 – 8 December 2022)

Contents

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and combating financing of terrorism (AML/CFT) measures in place in Estonia as at the date of the onsite visit (25 April -6 May 2022). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Estonia's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

a) Estonia has an appropriate mechanism for identification, assessment and, subsequently, understanding of ML/TF risks through national risk assessments coordinated by the AML/CFT Committee with high-level commitment and nationwide coverage, access to all data available in the country from public and non-public sources. Other strategic analysis products, also contribute to better understanding of risks in the respective sectors. While together those provide useful hints on sectors with higher risk exposure, they do not give a comprehensive view of the (residual) risks of ML and TF in the country. All competent authorities have a role in the implementation of the activities established under the national AML/CFT policy, i.e., most recent Action Plan. Nonetheless, outcomes of nation-wide risk assessment exercises are not integrated into the objectives and activities of individual authorities. National cooperation and coordination is a strong feature of the AML/CFT system in Estonia, supported by regular work of the high-level AML/CFT Committee, operational-level working groups/platforms, as well as adequate bilateral cooperation mechanisms and practices.

b) Financial intelligence along with other relevant information is gathered and used by the competent authorities to initiate and support ongoing investigations, to develop evidence and to trace criminal proceeds. Estonia should be commended for the demonstrated practice of co-ordination and co-operation between the EFIU and LEAs, and the EFIU's efforts to meet the operational needs of the LEAs. In recent years, important steps were made to strengthen the EFIU's capacities and its performance. A moderate improvement is still required in the EFIU's capacities and working practices for reinforcing its proactive approach in the detection of targets versus its current heavy reliance on the LEA's lead. This is a priority matter in the context of Estonia, as the EFIU is in the best position to observe and detect the movement of illicit flows. The competent authorities receive reports that contain relevant and accurate information that assists them to perform their duties to a moderate extent. This is due to issues with the quality and reporting practices of OEs. At the same time, some of the EFIU's practices raise concerns in terms of revealing the operational work done by the EFIU in respect to suspicious transactions and thereby jeopardizing the detection of crime and the tracing of assets.

c) In Estonia, different sources of information are used to trigger ML identification and investigation. While some significant cases involving banks are currently ongoing, the number of identified and investigated ML cases is relatively low mainly due to the limited interpretation of the ML offence by the Supreme Court. So far achieved results are to some extent in line with the risk profile of the country. Concerns remain regarding whether the risks relating to domestic high-proceeds-generating offences, are being sufficiently considered to investigate potential ML. The criminal sanctions applied for the ML offence call into question their dissuasiveness and effectiveness given the gravity and associated risk.

d) Confiscation is recognised as a policy objective in Estonia, but the achieved results follow the set objectives to some extent. Authorities achieved some reasonable results, however, proceeds of crime in specific cases were appreciably much higher than the amounts subject to confiscation. LEAs regularly conduct financial investigations, but authorities do not keep statistics and overall effectiveness is questionable. Estonia does not proactively pursue proceeds moved abroad. Sanctions applied for undeclared cash are minor unless amount exceeds EUR 40 000 when criminal proceeding is initiated. Confiscation results are not always in line with the risk profile of the country.

e) There has been one successful TF prosecution and conviction in Estonia which does not fully correspond to the risk profile of the country, and deficiencies in TF risk understanding (see IO.1) affect the overall effectiveness. Authorities use a range of sources of information and investigative techniques when identifying and investigating TF, yet EFIU disseminations and terrorism related offences alongside with financial investigations could be exploited more in order to determine potential TF offences. Features of TF investigations have been integrated to some extent in the counterterrorism strategy and Estonia makes effective use of alternative measures.

f) Estonia implements the UN TFS on TF and PF without delay. The mechanisms for designation of persons and entities under the UN TFS framework at the domestic level or internationally were not developed over the majority of the assessment period. No formalised approach was ensured to the designation process, including discussions and decision taking within the scope of a formal fora despite having potential causes to do so. Over the last year Estonia reinforced its attention towards implementation of the TFS measures, and demonstrated tangible progress also in supervisory efforts, primarily focusing at the most important sectors, banks and VASPs, for which Estonia should be commended. But further steps are required to improve understanding of UN TFS regimes by the OEs.

g) The efforts of authorities to conduct risk assessment of the NPO sector and identify the subset with higher level of vulnerability for the TF abuse are commendable, but major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including in identification of the specific subset of the NPOs, *inter alia* through analysis of a wider input data and

expansion of the scope of considerations. The risk-based measures with respect to NPOs are to be considerably improved.

h) The concerted effort of the supervisor undertaken in recent years to increase the quality and compliance of the sector is seeing some improvements as a result. The ML risk understanding, and the effectiveness of the preventive measures varies across the sectors. Banks, which represent one of the most material sectors, and non-bank FIs have a good understanding of their ML risks, whereas VASPs, CSPs and other DNFBPs demonstrated less comprehensive understanding. Understanding of TF risk is generally lower across all sectors. The effectiveness of the preventive measures is impacted by the level of ML/TF risk understanding demonstrated by the entities. For much of the period under review, most of the reporting has been carried out predominantly by banks (70%).

i) Both, the EFSA and the EFIU have revised their supervisory approach and increased capacity in order to address the emerging risks posed by the supervised sectors. The licensing process of the FIs by the EFSA is overall quite comprehensive, however, for much of the period under review, the EFIU's procedures were less effective, evident particularly in the VASP sector. The EFIU's actions implemented in 2021 appear to have a positive impact on VASPs licensing processes. The supervisory activity was not always carried out on a risk-sensitive basis. The powers to sanction unlicensed activity and to impose financial sanctions are limited. Overall, the applied sanctions cannot be considered to be effective, proportionate and dissuasive.

j) The authorities have taken certain steps towards identification, assessment and understanding of ML/TF vulnerabilities and risk exposure of legal entities. Nevertheless, the current understanding is not sufficient to take into account the existing risks. The competent authorities have powers to access information, but the measures to prevent misuse of legal persons do not fully enable availability of adequate, accurate and current BO information. The large share of Estonian companies with e-Residents as their basic or beneficial owners, significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information. Applicable sanctions are not effective.

k) MLA and extradition to EU and non-EU MS is provided in a constructive manner. Estonia has reserved the right to refuse assistance due to the principle of dual criminality, which hinders cooperation with non-EU jurisdictions. MLA is sought to pursue ML/TF and predicate offense investigations to some extent. There are few requests sent regarding seizing assets in foreign jurisdiction, and no information on confiscation of assets moved abroad. The extent to which other forms of international cooperation is sought and provided differs among authorities.

Risks and General Situation

2. Estonia faces money laundering (ML) threats from proceeds of crime primarily committed abroad and less frequently domestically. Estonia is considered to be a transit country for the concealment of ML and for the concealment or conversion of the origin of assets acquired by criminal activity. According to national risk assessment (NRA) the prevailing trends and patterns of ML involve the use of legal persons, money mules, wire transfers, cash deposits and withdrawals[1], and physical cross-border cash flows. Estonia is considered to be particularly exposed to threats related to fraud and internet fraud (embezzlement) committed abroad, as well as tax offences committed in the neighbouring countries. The authorities have also identified the laundering of illicit proceeds through drug trafficking, OCG, economic activities without an activity license.

3. Estonia is facing low level of terrorism threat. The threat level of terrorist financing in most domains is low in Estonia, it is average in the traditional financial sector and high in the VASP sector. In Estonia, threats posed by Islamist terrorism are the most likely. There is observation that TF is not related to predicate offences, and therefore they have been assigned by the lowest possible threat. The Internal Security Service's (ISS) annual report that provides the observation of situation in Estonia with respect to terrorist threat, suggests that people of Estonian origin still remain in the conflict zones[2]. The NRA conclusions suggest that country observes two sectors, the virtual asset service providers (VASPs) and non-profit organisations (NPOs) to be of higher vulnerability for TF. The VASPs are considered so due to the anonymity of the provided services. The NRA clarifies that TF risks can be higher with respect to the humanitarian and charitable activity carried out at international level near or within the conflict zones. According to the Action Plan the country considers that currently it has incomplete overview on the TF risks in the NPO sector, which is a vulnerability.

4. Banks and VASPs are the most vulnerable sectors in terms of ML due to (i) their dominating size, (ii) the spectrum of provided services, and the anonymity offered by the latter. Over the period under consideration there were AML/CFT shortcomings identified by the supervisor at four banks, out of which two are currently under criminal proceedings (see IO7). Among the DNFBPs the CSP and real estate are the most vulnerable sectors[3]. The CSP sector is vulnerable due to its current size and increasing number of participants, and the nature of the provided services[4], e.g., formation of companies for foreign residents. The real estate sector is vulnerable due to the risks attached to the real estate market itself, and involvement into the transactions of a real estate brokers (dealing with the transfer of cash to the customer's bank account)[5].

Overall Level of Compliance and Effectiveness

5. Estonia has taken steps since its last evaluation to remedy the deficiencies identified during that process – the jurisdiction strengthened its legal and regulatory framework and conducted its first NRA (covering the period from 2011 to 2013), which was adopted endorsed in January 2015

[1] NRA, National threat of ML and FT, pg. 4 and 6
[2] https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202020-2021.pdf
[3] NRA, Summary table with results of NRA.
[4] CSPs are among the biggest DNFPB sectors by the total turnover (around 50 million euros) comprising 316 participants (in 2020) identified as trust and company service providers. Their number significantly increased by almost three times when compared to 115 providers in 2017.
[5] NRA, Chapter 6 "Vulnerability of the real estate agents' sector", p.3

and published in March 2018. This was then updated covering the period 2017-2019, with the report endorsed in April 2021 and published in May 2021.

6. In many respects, Estonia demonstrated efforts toward developing an effective AML/CFT system, although the practical application of the existing framework has still to be improved. Notably, the country took steps to strengthen the supervisory efforts and demonstrated positive dynamic towards reinforcement of the banking sector and lately focused also on VASPs. Among other initiatives it is worth mentioning the revision of the EFIU status and provision with considerable additional resources, and Estonia's steps towards strengthening transparency of legal persons through development of the Beneficial Ownership Information Database (BOID) under the control of the Ministry of Finance.

In terms of technical compliance, the legal framework has been enhanced in many aspects, especially with respect to strengthening the requirements on application of preventative measures. Nevertheless, some issues remain, including measures applied with regard to: implementation of UN TFS (R.6-7); measures related to correspondent relationships (R.13); regulation of VASPs (R.15); application of preventative measures and supervision of DNFBPs (R.23 and R.28); reporting of STRs (R.20); statistics (R.33) and sanctions (R.35).

Assessment of risk, coordination, and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. Estonia has an appropriate mechanism for identification, assessment and, subsequently, understanding of ML/TF risks through national risk assessments, which should be significantly improved to provide for uninterrupted coverage of considered periods, as well as timely endorsement and dissemination of the assessment outcomes. The same is true for the action plans produced on the basis of NRA findings. While the NRA 2021 report and other strategic analyses provide useful hints on sectors with higher risk exposure, they do not give a comprehensive view of the (residual) risks of ML and TF in the country. There are also important missing elements in the understanding of ML/TF threats emanating from domestic proceeds-generating crimes, organized crime, cross-border movement of funds and cash, ML/TF vulnerabilities in private and public sectors, risks related to the abuse of legal persons, activities of CSPs and VASPs, as well as the country's exposure to the risk of terrorism financing. All competent authorities have a role in the implementation of the activities established under the national AML/CFT policy, i.e., most recent Action Plan. Nonetheless, outcomes of nation-wide risk assessment exercises are not integrated into the objectives and activities of individual authorities. National cooperation and coordination is a strong feature of the AML/CFT system in Estonia supported by regular work of the intergovernmental committees and adequate bilateral arrangements.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

8. Financial intelligence along with other relevant information is gathered and used by the competent authorities to initiate and support ongoing investigations, to develop evidence and to trace criminal proceeds, this mostly to pursue the ML predicate offences. Estonia should be commended for the demonstrated practice of co-ordination and co-operation between the EFIU and LEAs and the EFIU's efforts to meet the operational needs of the LEAs. In recent years, important steps were made to strengthen the EFIU's capacities and its performance. A moderate improvement is still required in the EFIU's capacities and working practices in order to reinforce its proactive approach in the detection of cases and to lessen its current heavy reliance on the LEA's lead. This is a priority matter in the context of Estonia, as the EFIU is in the best position to

observe and detect the movement of illicit flows by itself. However, this potential is greatly limited, among other things, by the low quality of reporting, which includes retroactive reporting. In addition, when the EFIU suspends funds, it informs the interested party of the suspension order and it practices in-person meetings with such parties in order to ascertain the origin of the funds (the latter having been addressed also in the 4th round of ME). These two matters raise concerns as may hamper the EFIU's and LEAs' efforts in tracing proceeds and detecting ML cases and predicate offenses.

9. Estonia has designated authorities to identify and investigate ML offence using mainly police reports and EFIU disseminations as a source. The interpretation of the ML offence by the Supreme Court in some cases has been narrower than the legislative threshold, thus hindering further investigations and prosecutions. So far, the achieved results are to some extent in line with the risk profile of the country. Estonia pursues different types of ML, and the majority of investigations, prosecutions and convictions for ML are for third party ML, usually in relation to foreign predicate offending. It is noticeable that Estonia has directed its resources and focused on complex ML cases. The sanctions for ML are not effective and dissuasive since they are low for natural persons and very low for legal persons, with imprisonment of natural persons usually suspended. Extended confiscation is used in cases where ML is not pursued but the reasons provided are not necessarily justifiable.

10. There is robust legislative framework enabling freezing, seizure and confiscation of instrumentalities and proceeds of crimes, confiscation of equivalent value, as well as extended confiscation. While confiscation is pursued as a policy objective, overall implementation in practice is achieved to some extent. There is a sizeable difference between estimated criminal property and that which is ultimately confiscated. The effectiveness of the confiscation in relation to the proceeds moved abroad is questionable. There are some technical deficiencies as regards movement of cash and BNI and applied sanctions for undeclared cash are not dissuasive. The confiscation results achieved so far do not appear to be fully consistent with the level of ML risk.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

11. Legal framework to fight TF has certain deficiencies concerning criminalisation of the TF offence. There has been one TF conviction in Estonia so far, which is to some extent consistent with the country's risk profile. The ISS has initiated five criminal investigations, which demonstrates authorities' skills and knowledge to deal with TF offence. Nevertheless, EFIU disseminations and terrorism related offences alongside with financial investigations could be more exploited in order to determine potential TF offences. TF investigations are integrated into the national strategies to some extent, but not used as basis to propose designations of terrorist and terrorist organisations. Criminal sanctions applied are not considered being effective. There are several alternative measures applied in Estonia when TF conviction is not possible to secure.

12. Estonia implements the UN TFS without delay. The mechanisms for designation of persons and entities, under the UN TFS framework were not developed over the majority of the assessment period. No person is designated either domestically or proposed to the UN, although there are convictions achieved and other circumstances are present to give raise to a more focused and formalised consideration of the subject.

13. Over the last year Estonia reinforced its attention towards the implementation of the TFS measures, and demonstrated tangible progress also in supervisory efforts, primarily focusing at the most important sectors, banks and VASPs, for which Estonia should be commended. Nevertheless, further steps are required to strengthen the OEs knowledge and capacities for

implementation of UN TFS, including by providing sector specific guidance, outreach and continuous regular supervision.

14. Estonia conducted risk assessment of the NPO sector within the framework of NRA in 2021 and a separate study by the EFIU in April 2022. These efforts of authorities are commendable, but major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including in identification of the specific subset of the NPOs, *inter alia* through analysis of a wider input data and expansion of the scope of considerations. The risk-based preventative measures with respect to NPOs are to be considerably improved.

Preventive measures (Chapter 5; IO.4; R.9–23)

15. Banking sector, which is weighted as one of the most important sectors, have a good level of understanding of their ML risks. Preventive measures in the banking sector are steadily improving since 2020 and there was a significant investment in AML/CFT compliance and risk management which enhanced the comprehensiveness of their mitigation controls. Most of reports come from the banking sector (70%). Throughout the period under review, this was not the case and four banks have committed serious AML/CFT violations. Since 2020, due to the supervisory measures a positive development is noted. This impacted the risk appetite of most banks which is limited for higher risk business. However, it is also observed a concentration of the risks within a small number of banks with higher risk appetite, mostly in relation to correspondent relationships with foreign high-risk business (VASPs, PSPs, EMIs and Fintech platforms) and VASP activity. One bank which also undertake VASP activity demonstrated a much weaker understanding of the risks and the mitigations put in place of VASP activity.

16. Generally, VASPs demonstrated a rather superficial understanding of risks and general mitigating measures applied. The preventive measures are often not applied in accordance with the specific business risk and the control systems are overall insufficient. At the same time, the reinforced supervisory attention towards the quality and compliance of the sector since 2020 indicate some positive results. VASPs had to adjust their business to higher licensing standards, including IT tools. Since 2019, as a result of the outreach activities the number of filed reports increased considerably, although a higher number is expected.

17. CSPs, demonstrated insufficient risk understanding and less effective preventive measures. The level of reporting by the sector is alarmingly low and the control systems are overall insufficient.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

18. The licensing process of the FIs by the EFSA is overall quite comprehensive, however, for much of the period under review, the EFIU's procedures were less effective, evident particularly in the VASP sector. The EFIU's actions implemented in 2021 appear to have a positive impact on DNFBPs and VASPs licensing processes. The SRBs assessment processes are much less thorough and undertake a limited assessment of the integrity of their members as shown by how few refusals or application withdrawals there have been since 2016.

19. The EFSA has comprehensive risk analysis tools which facilitate a good understanding of risks across the financial sector. Notwithstanding, the application of the risk methodologies, the EFSA should take into account and give appropriate weighting to all high-risk indicators to avoid assigning lower risk rating as would be expected which has a consequential impact on the effectiveness of the EFSA's supervisory approach. The EFIU's supervisory activity was not carried out on a risk-sensitive basis for the most period under review. This was mainly due to its

insufficient institutional capacity and limited understanding of the risks of the supervised sectors. Significant efforts have been made recently to address these weaknesses. The SRBs were able to explain some risks, however the explanations lacked depth or real appreciation of those risks with some matters being dismissed altogether without a convincing rationale.

20. The sanctioning mechanisms features a series of limitations, particularly regarding the ability to effectively impose financial penalties. The main supervisors rely heavily on remedial supervisory measures, such as warnings, remediation plans and licence withdrawal (where possible), and there are cases which would require more prompt supervisory actions. Overall, the applied sanctions cannot be considered to be effective, proportionate and dissuasive.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

21. The authorities have taken certain steps towards identification, assessment and understanding of ML/TF vulnerabilities and risk exposure of legal entities. Nevertheless, the current understanding lacks systematised and consolidated analyses and conclusions on important determinants and factors of risk, as well as on factually ascertained risks. The measures to prevent misuse of legal persons at the level of companies, OEs, competent authorities and registers do not fully enable availability of adequate, accurate and current BO information in the country. The large share of Estonian companies with e-Residents as their basic or BOs, significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information. Having regard to the significant presence and activities of non-licensed CSPs, the country has not made appropriate arrangements to raise awareness of OEs exposed to relationships with trustees and thus provide for adequate, accurate and current BO information on foreign trusts. There are no enforceable measures (for supervisors) or practices (for all competent authorities) to obtain basic and BO information from companies. Applied sanctions are not effective proportionate and dissuasive sanctions.

International cooperation (Chapter 8; IO.2; R.36–40)

22. In general, Estonia provides broad range of constructive MLA and extradition to EU and non-EU Member States in a constructive way. Prioritisation and timely execution of the request is ensured to some extent. Estonia has reserved the right to refuse assistance due to the principle of dual criminality, which hinders cooperation with non-EU jurisdictions. MLA is sought to pursue ML/TF and predicate offense investigations to some extent, while major improvements are needed when seeking assistance to seize and confiscate assets moved abroad. While some authorities have strong informal cooperation, deficiencies have been observed in the EFIU cooperation when performing supervisory role. Estonia provides basic and beneficial ownership (BO) information. While basic and BO information is provided to foreign counterparts, issues identified under IO.5 may hinder effectiveness of such cooperation.

Priority Actions

a) Estonia should take measures to significantly enhance the understanding of ML/TF risk faced by the country through, *inter alia*, improvement of nation-wide ML/TF risk assessments so as to provide for uninterrupted coverage of considered periods, timely endorsement and dissemination of relevant outcomes. Such outcomes should reliably assess ML/ TF threats and vulnerabilities, give a comprehensive view of the (residual) ML/TF risks in the country, and underlie appropriate nation-wide AML/CFT policies constituting effective and timely response to existing and potential risks

b) The EFIU should revise its capacities and working practices and reinforce a proactive approach in the detection of ML/TF targets on its own motion, including in high-risk areas, while continue providing support to LEAs within their ongoing proceedings. The EFIU should revise the quality of OE's reporting by revising the reporting guidelines, enhancing training and feedback to OEs. Estonia should ensure that: (a) the EFIU refrains from in-person meetings for obtaining additional clarifications about suspicious transactions from the party in question; and (b) the length of the EFIU suspension orders be adjusted so as to avoid raising the need to inform the customer about the application of this measure.

c) Estonia should expeditiously ensure that judiciary's and LEAs' interpretation of the ML offence is aligned with the international standards and domestic legislation. This should be approached by taking steps such as *inter alia*: (i) developing formal guidelines drawing on international and domestic requirements for ML offence and good practice for investigating and prosecuting ML offence; (ii) continuing to bring prosecutions in court and appealing decisions to promote evolving jurisprudence on ML cases in line with the current criminalisation of ML and international standards; (iii) holding regular training and seminars for judges, prosecutors and investigators.

d) Estonia should enhance to a major extent its efforts to seize, confiscate and recover the proceeds of ML and predicate offences, especially those moved abroad, in line with its ML/TF risks. The results should be periodically analysed in terms of their adequacy, the consistency with risks and any challenges, actual or potential, that the authorities have faced.

e) Estonia should ensure that TF activities are investigated and prosecuted in line with its improved understanding of national TF risks.

f) Estonia should ensure considering designations according to UNSCR at the domestic and international level collectively, in the formal fora, including formal consideration of whether the UN designation criteria are met with respect to persons under investigation or convicted, also irrespective of existence of criminal proceedings.

g) Authorities should strengthen ML and TF risk understanding across sectors (especially VASPs, CSPs and investment firms) and application of mitigating measures commensurate with their risks; ensure that independent verifications are undertaken by CSPs without undue reliance on other parties; enhance the control systems employed by VASPs and CSPs; ensure implementation of a travel rule and other newly established measures by VASPs; continue to ensure adequacy of

measure at OEs who also undertake VASP activity; continue supporting OEs for improving reporting level.

h) The supervisors should continue their efforts to ensure an effective licensing process of all OEs. They should undertake a comprehensive review of their risk-based approach to ensure that there is increased and proportionate focus on higher risk sectors and that there is appropriate focus on all higher risk matters. The existing supervisory arrangements in cases when an FI undertakes VASP activity should be clarified. The EFSA and EFIU should be given appropriate powers to sanction unlicenced activities and to impose effective, proportionate and dissuasive financial sanctions.

i) Estonia should more proactively seek international cooperation in order to pursue ML, as well as to support ongoing TF investigations. Particular attention should be given to seeking assistance regarding seizure and confiscation of assets moved abroad, mindful the fact that most proceeds are moved through Estonia to foreign jurisdictions.

j) The authorities should further develop the understanding of ML/TF risks related to the misuse of legal persons, including those arising from the e-Residency program. Such understanding should be achieved through, *inter alia*, systematised and consolidated analyses concluding on important determinants and factors of risk, as well as on factually ascertained risks. Measures should be taken to improve the quality of BO information in the country, including through more effective contribution by companies and OEs, and through consistent efforts by relevant authorities in conducting proactive checks and verification of company information.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[6]

IO.1 – Risk, policy and coordination	IO.2 – International cooperation	IO.3 – Supervision	IO.4 – Preventive measures	IO.5 – Legal persons and arrangements	IO.6 – Financial intelligence
Moderate	Substantial	Moderate	Moderate	Moderate	Substantial
IO.7 – ML investigation & prosecution	**IO.8 – Confiscation**	**IO.9 – TF investigation & prosecution**	**IO.10 – TF preventive measures & financial sanctions**	**IO.11 – PF financial sanctions**	
Moderate	Moderate	Moderate	Moderate	Substantial	

Technical Compliance Ratings[7]

R.1 - assessing risk & applying risk-based approach	R.2 - national cooperation and coordination	R.3 - money laundering offence	R.4 - confiscation & provisional measures	R.5 - terrorist financing offence	R.6 - targeted financial sanctions – terrorism & terrorist financing
PC	C	LC	C	LC	PC
R.7- targeted financial sanctions - proliferation	**R.8 -non-profit organisations**	**R.9 – financial institution secrecy laws**	**R.10 – Customer due diligence**	**R.11 – Record keeping**	**R.12 – Politically exposed persons**
PC	PC	C	LC	C	LC
R.13 – Correspondent banking	**R.14 – Money or value transfer services**	**R.15 – New technologies**	**R.16 – Wire transfers**	**R.17 – Reliance on third parties**	**R.18 – Internal controls and foreign branches and subsidiaries**
PC	LC	PC	C	LC	LC
R.19 – Higher-risk countries	**R.20 – Reporting of suspicious transactions**	**R.21 – Tipping-off and confidentiality**	**R.22 - DNFBPs: Customer due diligence**	**R.23 – DNFBPs: Other measures**	**R.24 – Transparency & BO of legal persons**
PC	PC	PC	LC	PC	PC
R.25 - Transparency & BO of legal arrangements	**R.26 – Regulation and supervision of financial institutions**	**R.27 – Powers of supervision**	**R.28 – Regulation and supervision of DNFBPs**	**R.29 – Financial intelligence units**	**R.30 – Responsibilities of law enforcement and investigative authorities**
PC	LC	LC	PC	LC	C
R.31 – Powers of law enforcement and investigative authorities	**R.32 – Cash couriers**	**R.33 - Statistics**	**R.34 – Guidance and feedback**	**R.35 - Sanctions**	**R.36 – International instruments**
C	LC	PC	LC	PC	LC
R.37 – Mutual legal assistance	**R.38 – Mutual legal assistance: freezing and confiscation**	**R.39 – Extradition**	**R.40 – Other forms of international cooperation**		
LC	LC	LC	LC		

[6] Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.
[7] Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

MUTUAL EVALUATION REPORT

Preface

1. This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 25 April to 6 May 2022.

3. The evaluation was conducted by an assessment team consisting of:

Assessors

Mr André Reber – Deputy Section Head, Financial Analyst II, Operational Analysis Confederation, Division MROS, Federal Office of Police, Switzerland (law enforcement expert)

Mr Arakel Meliksetyan – Head, Financial Monitoring Center, Central Bank of Armenia (financial expert)

Mr Daniel Johnson – Senior Manager of Policy and Authorisations, Isle of Man Financial Services Authority (financial expert)

Ms Diana Rocco – Head of the Financial Information Office of the Supervisory and Financial Information Authority Holy See (including Vatican City State) (law enforcement expert)

Mr Steven Meiklejohn – Advocate and Legal Adviser in His Majesty's Law Officers' Department Jersey (legal expert)

Mr Vidar Gothenby – Senior Legal Counsellor, Finansinspektionen, the Swedish Financial Supervisory Authority (legal expert)

MONEYVAL Secretariat

Ms Ani MELKONYAN – Administrator

Ms Ana Boskovic – Administrator

Ms Stela BUIUC – Administrator

4. The report was reviewed by Mr Tobias Ligaard Brynildsen (Norway), Mr Rizumu Yokose (Japan), Mr Lajos Korona (MONEYVAL Scientific Expert) and the FATF Secretariat.

5. Estonia previously underwent a FATF Mutual Evaluation in 2014, conducted according to the 2004 FATF Methodology. The 2014 evaluation report and 2019 follow-up report have been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/estonia.

6. That Mutual Evaluation concluded that the country was compliant with 8 Recommendations; largely compliant with 28; partially compliant with 12; and non-applicable with 1. Estonia was rated largely compliant with 11 of the 16 Core and Key Recommendations. In July 2019, Estonia exited the follow–up process on the basis that it had reached a satisfactory level of compliance with Core and Key Recommendations in line with Rule 13, para. 4 of MONEVAL's Rules of Procedure.

1. ML/TF RISKS AND CONTEXT

1.1. ML/TF Risks and Scoping of Higher Risk Issues

1. Estonia is situated in the northern Europe, on the eastern shore of the Baltic Sea. Estonia is bordered to the north by the Gulf of Finland dividing the 80 km from Finland; to the west by the Baltic Sea across from Sweden, to the south by Latvia, and to the east by Lake Peipus and Russia. Its territory of 45,339 km^2 consists of 15 counties shared by 79 local governments, but the population density is largely concentrated in the capital area of Tallinn[8]. Estonia joined the European Union on 1 May 2004 and became a member of the Schengen Area on 21 December 2007. Estonia adopted the Euro as currency on 1 January 2011.

2. Estonia is among the smallest Member States of the European Union with a population of 1 331 769 inhabitants (2022). The structure of the Estonian economy has been relatively stable, with certain trends indicating the continuous modernisation both in terms of importance of the public sector and the structure of private sector. Estonian GDP was EUR 30.7 billion and GDP per capita was EUR 23 060 (at current prices) in 2021.

3. The Estonian economic structure has been mainly service-oriented over the period of 2015-2021, the most important sectors are trade, repairs, transport, accommodation and food services with 20.5% of the GDP; industry (incl. energy) with 19.2% and public administration, defence, education, health and social work (16.7%). The other economic sectors remain below 10%, where the relative importance of information and communication has grown over the years (from 5.5% in 2015 to 8,6% in 2021), as has the financial services sector, though in a slower pace (from 4.4% to 4,6%, respectively). Professional, scientific, support services and real estate sectors constituted 9.6% and 9.7% of the GDP in 2021, construction 6.6% and remaining 2.5% were assigned to agriculture, forestry and fishing and 2.7% to other services.

4. Estonia is a parliamentary republic with a single-chamber parliament (Riigikogu) and a civil law legal system based on the Germanic legal model. The Estonian parliament has 101 members elected in general elections for a four-year-term and it has the right to appoint high officials of the state, including the President of the Republic and the Prime Minister, as well as to approve the members of Government. The government carries out the country's domestic and foreign policy, shaped by parliament; it directs and co-ordinates the work of government institutions and bears full responsibility for everything occurring within the authority of executive power.

5. Estonia is actively participating in various international organisations, EU agencies and bodies: having recently completed its first presidency in the United Nations[9] Security Council (in 2020-2021), the country is a member in The Organisation for Economic Co-operation and Development (OECD)[10], and Council of Europe[11] and their various bodies, as well as Egmont

[8] 69% of people live in towns, out of which 40% live in Tallinn area.
[9] After regaining its independence Estonia joined the UN 17.09.1991
[10] 9.12.2010
[11] 14.05.1993

Group, International Monetary Fund (IMF), World Bank, World Trade Organization (WTO), European Bank for Reconstruction and Development (EBRD), International Criminal Police Organization (INTERPOL), European Union Agency for Law Enforcement Cooperation (EUROPOL) and European Public Prosecutor's Office. Estonian Financial Supervisory Authority (EFSA) is part of European Supervisory Authorities (ESA), including European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA) and European Banking Authority (EBA), and is also in the Single Supervisory Mechanism (SSM).

1.1.1. Overview of ML/TF Risks

6. Estonia faces money laundering (ML) threats from proceeds of crime primarily committed abroad and less frequently domestically. Estonia is considered to be a transit country for the concealment of ML and for the concealment or conversion of the origin of assets acquired by criminal activity. According to national risk assessment (NRA) the prevailing trends and patterns of ML involve the use of legal persons, money mules, wire transfers, cash deposits and withdrawals[12], and physical cross-border cash flows. Estonia is considered to be particularly exposed to threats related to fraud and internet fraud (embezzlement) committed abroad, as well as tax offences committed in the neighbouring countries. The authorities have also identified the laundering of illicit proceeds through drug trafficking, OCG, economic activities without an activity license.

7. Estonia is facing low level of terrorism threat. The threat level of terrorist financing in most domains is low in Estonia, it is average in the traditional financial sector and high in the VASP sector. In Estonia, threats posed by Islamist terrorism are the most likely. There is observation that TF is not related to predicate offences, and therefore they have been assigned by the lowest possible threat. The Internal Security Service's (ISS) annual report that provides the observation of situation in Estonia with respect to terrorist threat, suggests that people of Estonian origin still remain in the conflict zones[13]. The NRA conclusions suggest that country observes two sectors, the virtual asset service providers (VASPs) and non-profit organisations (NPOs) to be of higher vulnerability for TF. The VASPs are considered so due to the anonymity of the provided services. The NRA clarifies that TF risks can be higher with respect to the humanitarian and charitable activity carried out at international level near or within the conflict zones. According to the Action Plan the country considers that currently it has incomplete overview on the TF risks in the NPO sector, which is a vulnerability.

8. The NRA identifies that the restrictive interpretation of the ML set by the Supreme Court decisions[14], lengthy judicial proceedings, and capacity of competent investigative authorities are important vulnerabilities. Based on the NRA findings[15], as also confirmed by the open-source information the use of various types of wire transfer services, use of cash and purchase of real estate are ML vulnerabilities. Banks and VASPs are the most vulnerable sectors in terms of ML due to (i) their dominating size, (ii) the spectrum of provided services, and the anonymity offered by the latter. Among the DNFBPs the CSP and real estate are the most vulnerable sectors[16]. The

[12] NRA, National threat of ML and FT, pg. 4 and 6
[13] https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202020-2021.pdf
[14] Supreme Court judgement No. 3-1-1-34-05, Supreme Court decision No. 1-15-6497
[15] NRA, p.19
[16] NRA, Summary table with results of NRA.

CSP sector is vulnerable due to its current size and increasing number of participants, and the nature of the provided services[17], e.g., formation of companies for foreign residents. The real estate sector is vulnerable due to the risks attached to the real estate market itself, and involvement into the transactions of a real estate brokers (dealing with the transfer of cash to the customer's bank account)[18].

1.1.2. Country's Risk Assessment & Scoping of Higher Risk Issues

9. Estonia conducted its most recent national ML/TF risk assessment in 2020, using the WB methodology, which was adjusted to fit peculiarities of the country. The AML/CFT Committee[19] chaired by the Minister of Finance and comprised of the high-level representatives of ministries[20], law enforcement and oversight agencies[21], financial supervisors[22] and the national financial intelligence unit coordinated preparation and conduction of the NRA. The NRA Steering Committee overseen by the AML/CFT Committee organised, planned and coordinated the assessment process in accordance with the methodology. Throughout that process, ten different working groups with around eighty experts representing public agencies, umbrella organisations and private companies contributed to the NRA. The report of the national risk assessment mostly covering the period 2017-2019 was endorsed by the AML/CFT Committee on 28 April 2021 and published on the MOF website on 25 May 2021.

10. In the course of conducting the assessment, the authorities identified a number of shortcomings of the methodology and the assessment process regarding, *inter alia*, insufficient data on important sources of threats, contradictory criteria for assessing possible consequences of threats, weak and theoretical knowledge of the competent authorities about TF threats, as well as other issues of organizational and substantial nature. As further explored under Immediate Outcome 1, in addition to this, the AT identified significant shortcomings with the application of the NRA methodology and the outcomes of the assessment regarding, first of all, the disconnect – due to the lack of comprehensive analysis and substantiated judgments – between quantitative and qualitative indicators of threat and vulnerability factors on one hand, and the ratings determined for these factors to calculate threat and vulnerability scores on the other hand. Accordingly, the conclusions of the NRA 2021 report do not appear to be a reliable assessment of the ML/TF threats and vulnerabilities in the country. Moreover, the NRA 2021 report, including its Executive Summary, does not set out conclusions on ML/TF risks, as it reflects on threats and vulnerabilities assessed descriptively (high, above average, average, below average, and low) and numerically (on a scale of 1 to 5), which nevertheless do not give a comprehensive view of the (residual) risks of ML and TF in the country.

11. Among other systematised risk assessment exercises in the country, one should mention the sectorial risk assessment conducted by the EFSA, mostly covering the period 2014-2020 and

---

[17] CSPs are among the biggest DNFPB sectors by the total turnover (around 50 million euros) comprising 316 participants (in 2020) identified as trust and company service providers. Their number significantly increased by almost three times when compared to 115 providers in 2017.
[18] NRA, Chapter 6 "Vulnerability of the real estate agents' sector", p.3
[19] The committee was established on 19 April 2018 by Regulation No. 34 of the Government of Estonia.
[20] The Ministry of Finance, the Ministry of the Interior, the Ministry of Foreign Affairs, the MEAC, and the MoJ.
[21] The Internal Security Service, the Police and Border Guard Board, the Tax and Customs Board, and the Public Prosecutor's Office
[22] The Estonian Financial Supervision Authority and the Eesti Pank.

endorsed by the EFSA Board on 24 May 2021, i.e., almost simultaneously with the NRA 2021 report. The EFSA has not published the SRA report. As further explored under R.1, similarly to the NRA report, the SRA report does not set out conclusions on ML/TF risks, but rather reflects on threats and vulnerabilities in the financial sector descriptively assessed on a 4-level scale (low, medium, high and very high). While not anticipating use of identical methodologies for the NRA and the SRA, the assessment team notes that the differences between these two same-age risk assessment exercises – at least in the way that the findings on identified and assessed constituents of risk are formulated – makes it difficult to conclude on the extent of reconciliation and alignment of their outcomes. Other shortcomings of the SRA analysis and outcomes are related to the use of contradictory statistical data; circular references to other reports or sources of information; statements not supported by any statistical data or expert judgments; lack of reliable estimates on domestic proceeds of crime and cross-border movements of funds potentially related to ML, etc.

12. The EFIU has also conducted thematic analyses, such as the 2020 and 2022 surveys on VASPs, the 2021 study of ML risks related to CSPs, and the 2022 overview of the NPO sector. As further explored under Immediate Outcome 1, these analyses are a good beginning for identification and assessment of ML/TF risks in the respective sectors, which needs to be further developed in the course of future iterations in order to fill the remaining gaps in the understanding of risk (e.g., the analysis regarding the number of clients, the volume of transactions, as well as internal controls, including risk classification of customers and application of CDD measures applied by VASPs is based merely or predominantly on the data presented by service providers, which responded to the EFIU questionnaire; or, the NPO overview does not specify how exactly the NPOs have been identified as the ones which, by virtue of their activities or characteristics, are likely to be exposed to a higher risk of TF abuse).

13. In their preparatory work, the assessors identified several topics requiring additional attention. To do this, they analysed the ML and TF risk assessments presented by the Estonian authorities and took note of the information available on the legal and institutional environment and the context of ML/TF risk in Estonia, including points of potential vulnerability.

14. Particular attention was paid to the following issues during the on-site visit, and this is reflected in the analysis in the report:

15. ***E-Residency:*** Estonia is the first country in the world to provide e-Residency. E-Residency provides opportunities for establishing a legal person (including NPOs) in Estonia remotely, managing it, signing documents, and conducting bank transactions, including running their local businesses via internet[23]. Between 2014 and 2021 there were in total 76 070 e-Residency status acquirers (top 5 citizenships are Finland, Russia, Ukraine, Germany, and China), and 15 907 legal persons setup by e-Residents. The authorities identified the following important risks related to this product: Estonia cannot obtain reliable information on applicants from the non-EU member states or effectively prosecute their offenses later. The e-Residence can be abused by committing offenses with a digital ID, including fraud, tax fraud, financial crime, ML, and organised crime or TF, or concealing the real user - giving a digital ID to another person for use. Estonia envisaged implementation of a number of national measures aimed at minimising ML/TF risks related to

[23] NRA, "4.3. Analysis of risks related to the e-Residency programme", p.1

misuse of e-Residency. The evaluation team has focused on effectiveness of detection of related risks and their mitigation in the context of AML/CFT efforts in various fields (supervision, preventative measures, transparency of legal persons and arrangements, law enforcement proceedings and international cooperation).

16. ***VASPs*:** The sector is attractive and misused for criminal purposes. Over the past period under review of the evaluation team a large number of companies setup by the CSPs, that obtained the VASP licenses were sold to e-residents and non-residents. Most of the actual business operations, board members, BOs and customers of the companies with a licence issued in Estonia are located abroad. The higher ML/TF risk associated with VA determined more stringent requirements introduced in 2020 to VASPs and led to revocation of a total of 1808 licenses. The recent measures have not proven to be sufficient, according to the NRA[24] and the Government approved (on December 23, 2021) further legislative amendments to more effectively regulate VASPs to mitigate the risk of financial crime[25]. The evaluation team has explored: (i) the market entry controls in place, including fit and proper assessment; (ii) supervisory practices, understanding of the market participant's individual risks, especially where the services are provided abroad; (iii) effectiveness of risk mitigating measures implemented by the county on the basis of the risk assessment of the VASP sector; (iv) the interaction between the VASP and financial sectors, including risk understanding and mitigating measures implemented by the FIs providing services to VASPs; (v) coverage of the markets that the VASPs are providing services to, associated risks and mitigating measures; and (vi) effectiveness of national cooperation among the competent authorities and public-private partnership.

17. ***Banking sector:*** Within the financial sector banking sector is the most material one. According to NRA findings, ML using bank accounts is the most popular method in Estonia employed by perpetrators[26]. Local branches of Nordic banks have been involved in large-scale ML schemes[27]. Banks are exposed to ML/TF risks associated with non-residents and e-residents[28], including those with no or only apparent connection with Estonia (e.g., company registered in Estonia), remote on-boarding and transactions (over 99% of all banking transactions in the country are carried out online[29], which pose an inherent risk for the banking sector to be misused by the criminals). Effectiveness of implementation of CDD measures is affected by difficulties in identification of BO, especially when related to complex ownership structure and digital movement of assets, and a PEP status of a customer.

18. Over the period under consideration AML/CFT shortcomings were identified by the supervisor at four banks: (i) first bank was closed and a criminal investigation initiated with the proceedings under was (see Bank D case in IO7), (ii) second bank was not closed but criminal

---

[24] NRA, page 3.
[25] https://www.fin.ee/en/news/estonia-tighten-regulation-virtual-asset-service-providers
[26] NRA, "3.1.1 Nature of predicate offences to money laundering and extent of money laundering in Estonia", p.3-4
[27] https://www.occrp.org/en/investigations/newly-obtained-audit-report-details-how-shady-clients-from-around-the-world-moved-billions-through-estonia; and https://www.theguardian.com/business/2022/jan/04/swedbank-ex-chief-birgitte-bonnesen-charged-baltics-money-laundering-scandal
[28] This is also confirmed by cases where deficiencies in identifying and managing the ML risk deriving from non-resident and resident customers with not resident owners were found in one of the largest banks: https://www.occrp.org/en/daily/12651-swedish-seb-bank-fined-for-poor-anti-money-laundering-measures
[29] https://e-estonia.com/solutions/ease_of_doing_business/e-banking/

investigation are in progress (see Bank S case in IO7), (iii) the findings on the third bank initially raised suspicion of criminal conduct, but further analysis of the case did not prove so and the supervisory proceedings were applied[30], and (iv) forth bank was closed by the supervisor without investigation in 2018[31] this was not a material one compared to the other banks. As a result, the evaluation team closely examined the contributing factors to these failings and the effectiveness of mitigation/remedial measures. In addition, the focus of the evaluation team has been on: (i) banks' abilities to effectively mitigate the ML/TF risks through risk understanding and application of risk-based internal controls and preventive measures, including the effective implementation of group-wide policies and procedures, where relevant; (ii) implementation and adequacy of the CDD measures, including identification of BO, in particular where the customers have an e-resident status; (iii) of supervisory response to timely identification of weaknesses in the system, including fit and proper measures for detection of criminals and their associates, and application of corrective measures; (iv) effectiveness of guidance and training provided to the sector for improving its capacities.

19. ***Transparency of legal persons:*** Legal persons registered in Estonia are increasingly used in ML schemes[32]. In 2019 almost half (200) of STRs submitted by Notaries were related to the establishment of companies and transactions with shares[33]. The authorities have observed an increasing tendency of establishing Estonian companies with a non-resident BOs. Non-residents and e-residents can also easily and affordably establish companies in Estonia, acquire them from the CSPs, or from resident individuals who can provide such services against a fee (as demonstrated by the ML cases), thus creating an apparent connection with Estonia. Estonia identified that the Commercial Register (CR) does not always contain reliable basic and BO information as there is no mechanism for verification of submitted data, its timeliness and accuracy, especially when with a foreign or complex ownership. The evaluation team has analysed the effectiveness of mechanisms aimed at ensuring the transparency of legal persons in Estonia, and the extent to which accurate and up-to-date basic and BO information from various sources (public and private sectors) is available to competent authorities on a timely basis.

20. ***Company Service Providers (CSPs)*****:** While the NRA reflects on the risks related to CSPs, Estonia still concludes that there is a major lack of state awareness of the situation in this sector. The sector is characterised by serving foreign customers and is associated with the risk of exploitation of companies by criminal offenders (e.g., services for selling shelf companies to non-residents and e-residents; acquisition of companies for use as shell companies; use of nominee services for hiding the BO). Some of the CSPs were found to be involved in criminal cases or associated with criminals and the license has been revoked in two cases. While the Estonian legislation does not recognise trust, the CSPs are granted with a license for providing also trust services[34], as required by the EU regulatory framework. There is no risk analysis available on this issue in the NRA. The NRA identifies substantial deficiencies of the sector regarding the ML/TF risk understanding, implementation of the AML/CFT requirements, coupled with the avoidance of application of CDD measures (apparent non-establishment of a business relationship) and

[30] https://news.err.ee/1106263/seb-fined-1-million-over-money-laundering-prevention-deficiencies
[31] https://www.intellinews.com/estonia-s-versobank-closed-down-over-money-laundering-allegations-138937/
[32] NRA, "4.2. Analysis of the misuse of legal persons", p.2
[33] Ibid.
[34] An example of a company from the Registry: MTR (mkm.ee)

reporting obligations, and general lack of sufficiently qualified staff in the sector. The evaluation team has considered: (i) whether the risks attached to CSPs are understood properly by the country and the sector itself; (ii) how effective is a supervisory regime and response; (iii) efforts made aiming at improving the awareness of AML/CFT obligations by the sector, and (iv) ease, accuracy and timeliness of disclosure of basic and BO information to competent authorities.

21. ***Real estate market:*** Investment of proceeds of crime (including funds originating from cryptocurrencies) into the real estate is one of the common ML schemes. This found a confirmation in the STRs filed by notaries and detected criminal cases. More than half of the STRs submitted by notaries in 2019 (66%) concerned real estate transactions in total amount of approx. 60.62 million euros. Criminal cases highlighted involvement of foreign proceeds as a common pattern. The real estate market gatekeepers are real estate brokers, notaries and banks. While participation of the real estate broker, and a bank is not mandatory, a notarial verification of the transaction is obligatory. Use of cash in transactions also effectively reduces the involvement of banks. The real estate brokers nevertheless are dealing with the transfer of cash to the customer's bank account, thus potentially impacting on the effective performance of the preventative measures by banks. Risks are higher in relation to rental transactions of immovable property, where the involvement of notarial services is not mandatory. The NRA suggests that real estate brokers have a low level of awareness of their AML/CFT obligations and insufficient resources for their implementation. Notaries are found to have a higher effectiveness in implementation of their AML/CFT obligations. The evaluation team has focused on country's understanding of ML/TF risks in the sector, and adequacy of taken measures, e.g., for reducing the use of cash in the purchase of real estate; level of the supervisory attention to the real estate transactions when conducting inspection in the three types of reporting entities; measure taken to enhancing the knowledge and performance of their AML/CFT obligations by the real estate brokers.

22. ***ML investigation, prosecution and conviction:*** The analysis of the ML cases in the NRA suggests that these are mostly related to foreign predicate crimes, which are latter spread through Estonian financial system via bank accounts of companies or natural persons.[35] Estonia prioritises ML cases where there is negative impact to the state. There is little evidence that the domestic predicate offences led to investigation of ML. such as, e.g., illicit trafficking in narcotic drugs and psychotropic substances; fraud; and sexual exploitation[36]. The open-source information suggests that organised crime and human trafficking are also important threats present in Estonia[37]. According to the NRA outcomes and other international reports domestic corruption is not a systemic issue in Estonia. Nevertheless, in January 2021 the prime minister of Estonia resigned as his party and five individuals were suspected of involvement in "possible corruption" in relation to allegations of influence peddling and bribery over a property development project[38]. The lengthy judicial proceedings lead to the prevention of conviction in complex criminal cases[39]. In addition, the NRA Action Plan highlights that there are legal obstacles

[35]NRA, National threat of ML and FT, pg. 14
[36] The Mutual Evaluation Questionnaire statistics.
[37] Criminality in Estonia - The Organized Crime Index (ocindex.net); Estonia - United States Department of State; Estonia - The World Factbook (cia.gov)
[38] https://kyc360.riskscreen.com/news/juri-ratas-resigns-as-estonian-prime-minister-amid-corruption-scandal/
[39] Estonian Court's Red Tape Hinders Graft Case (occrp.org)

for ML proceedings[40] as well as restricted interpretation of ML offence by jurisprudence. FIs and the VASPs are frequently abused by the criminals for the purpose of ML[41]. The evaluation team has focused on: (i) the extent to which the competent authorities understand domestic ML risks; (ii) how well the competent authorities identify (including through parallel financial investigations), investigate, prosecute and convict ML with domestic and foreign predicate offences, including large-scale regional ML cases; (ii) the reasons for the lengthy judicial proceedings, their impact and measures taken for improving the system; (iii) the nature of legal obstacles such as the restrictive interpretation of the ML offence, the impact of these and measures taken or planned to address the same; (iv) the capacities and knowledge of the competent investigative and supervisory authorities and the FIU for timely and effective detection of crime committed by use of sophisticated products offered by FIs and VASPs, including crypto-gaming[42] and complex schemes; and (v) effectiveness of cooperation between competent LEAs FIs and VASPs in relation to the initiation of investigation of autonomous ML offence, especially for cases where predicate offences were committed abroad.

23. ***TF detection, criminal proceedings and mitigation:*** According to the statistics provided by the country, there have been 2 investigations, 1 prosecution and 1 conviction in the review period. Moreover, authorities reported that they received only 2 requests for MLA related to TF. While some external sources suggested that there were 4 foreign citizens expelled on the suspicion of involvement in jihadist terrorism[43] and operation Feuerkrieg Division terrorist group led by an Estonian national[44], there is no in-depth analysis available with this regard. It is not apparent that authorities considered migrant smuggling, organised crime, drug trafficking and trafficking in human beings and FTFs as potential TF threats. Authorities suggest that the high value of cross-border payments in Estonia and the anonymity of the services provided by the VASPs represent an elevated risk for the Estonian financial system to be misused for the purpose of TF[45]. At the same time the impact of the issues related to detection of a BO information either at the stage of company formation or providing financial or non-financial services does not seem to be sufficiently analysed as a TF vulnerability that can affect effective implementation of the risk-based and rule-based (i.e., TFS) requirements. The evaluation team has therefore explored: (i) the extent to which potential TF risks are well understood and addressed by the competent authorities; (ii) the extent to which the competent authorities cooperate and collaborate effectively and whether the overall criminal enforcements measures have proven effective; (iii) results are consistent with the jurisdiction's risk profile; (iv) how well the mechanisms for listing persons according to UNSCRs are functioning; (v) the level of the NPO sector vulnerability for the TF abuse overall, and the NPOs with heighten vulnerabilities in particular, and also the mitigating measure in place; (vi) the extent to which the OEs are provided by the supervisors and the FIU with tools for detection of TF suspicion and implementation of the

[40] Measure no.17 in the NRA Action Plan
[41] Ten Danske bank managers charged over ML - https://www.occrp.org/en/daily/9706-ten-danske-bank-managers-charged-over-money-laundering; Swedbank Saga - Nordic Noir: Understanding the Swedbank Saga (riskscreen.com); Swedish SEB Bank Fined for Poor Anti-Money-Laundering Measures - Swedish SEB Bank Fined for Poor Anti-Money-Laundering Measures (occrp.org);
[42] https://news.err.ee/1608443264/epl-tallinn-based-crypto-currency-gaming-firm-makes-pandora-papers
[43] EU Terrorism Situation and Trend Report, pg. 49
[44] https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442
[45] https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202020-2021.pdf

UN TFS and how effectively the OEs implement these; (vii) effectiveness of the mitigating measures in place for preventing abuse of the VASPs for the TF purposes.

24. ***Seizing, freezing and confiscation***: The NRA Action Plan highlights that there is no estimation of the proceeds of crime as well as lack of capacity to identify these. While some figures are available for application of seizure and confiscation, no information on effective confiscation achieved by the country is available. The proceedings with respect to assets held by legal persons are affected by the legislative advantage for them to initiate liquidation regardless of the initiation of criminal proceedings. Therefore, the evaluation team has analysed: (i) the circumstances and the extent to which financial investigations are carried out to detect the proceeds of crime; (ii) the extent to which the authorities are able to identify, trace, seize, confiscate and recover the proceeds of crime including ones that were moved abroad; (iii) the practice of confiscation of various types of assets (including virtual assets), (iv) the extent to which liquidation of legal persons during criminal proceedings affects the effectiveness of the confiscation regime; (v) Estonia's asset management practices.

25. ***MLA and international cooperation:*** Estonia identified that foreign predicate offences frequently feature in domestic ML cases. At the same time in the ML scheme proceeds of crime are also circulated through the Estonian FIs. This cross-border profile of criminal schemes entails that robust MLA mechanisms and other forms of international cooperation are essential for Estonia. The evaluation team has looked closely at the manner in which and effectiveness to which Estonia provides MLA and co-operates with foreign partners also though other means in the EU framework and outside of it. Seeking international assistance in a proactive manner has been also analysed. Considering that the financial market in Estonia including the VASPS are dominated by foreign capital, the assessment has focused also on the effectiveness of co-operation between domestic and foreign supervisory authorities[46]. In addition, taking into consideration the cross-border profile of legal persons registered in Estonia cooperation with foreign jurisdictions in respect to transparency of legal persons, accuracy and timely access to basic and BO information has been one of the focus areas of the evaluation team.

26. ***Sanctioning regime:*** As highlighted by the NRA, the lack of an administrative fine as a sanction continues to have a negative effect on the efficiency of supervision of preventive measures. Insufficient maximum fines based on misdemeanour proceedings also continue to be problematic. The evaluation team has considered how the effectiveness of sanctions is achieved through application of additional measures of enforcement to ensure effectiveness and dissuasiveness of sanctions for breaches of the AML/CFT obligations. In addition, fines imposed to legal and natural persons also in criminal proceedings are not dissuasive nor effective. On the contrary, imposed custodial sentences seem to be dissuasive. The evaluation team has considered whether imposed custodial sentences are proportionate and effective to the gravity of the

[46] NRA, Actual business operations, board members, beneficial owners, and also customers are located abroad. All this renders difficult supervision and processing of cases with necessary elements of a criminal offence. At the same time, the large number of companies with an activity license brings about a high risk of reputational damage for Estonia and there is no practical benefit for the Estonian state in hosting companies with activity licenses in its register. Due to the above, exploitation of virtual currency service providers in criminal schemes became commonplace and Estonia began to receive hundreds of foreign inquiries from other FIUs or law enforcement agencies, requesting information to identify and prove criminal offences committed by companies registered in Estonia.

committed crime, and whether the combination of these two types of sanctions effectively overcome the gap.

1.2. Materiality

27. Estonia is an open economy ranking 25th in the EU and 99th in the world based on total GDP (EUR 27,4 billion in 2020)[47]. The Estonian financial sector is relatively small. There are 15 banks, 5 of which operate as branches of foreign banks. Total bank assets amounted EUR 45 billion (21st in the EU) equivalent to 164% of the country's GDP[48] in 2020. The financial sector is concentrated and bank-focused (approximately 85% of total assets in 2021, followed by 10% fund management and 4.1% insurance), with around 94% of the total assets of the banking sector held by four largest banks. The authorities advise that the value of cross-border payments through Estonian banks was approximately EUR 95 billion in 2021, thus placing it the 11th among EU countries when relating the value of cross-border payments to population. There are also 16 PSPs with 9 of them providing payment services. The PSP sector is also concentrated, with one PSP (a payment solutions provider for e-shops) accounting for 60% of the total value of payment transactions at EUR 570 million in 2021, including EUR 113 million in cross-border payments.

28. According to the IMF definition of financial centers[49], Estonia does not classify as an international, regional or offshore financial center. Reports of the Financial Stability Board[50] (formerly the Financial Stability Forum) on adherence to regulatory and supervisory standards have not identified the country as ranking highly in financial importance. Nevertheless, important stakeholders in the private sector, such as Finance Estonia[51], pose the country as a future-facing financial center[52], taking consistent steps to raise awareness of the advantages of its financial sector in two focus areas: financial sector development and financial services export. On the other hand, in preparation of the current round of mutual evaluation of Estonia the authorities have analysed most recent MERs[53] of jurisdictions considered to be well-established or emerging financial centers, with reference to certain characteristic features used to identify such centers. Based on this analysis, the authorities support the opinion that the country is neither an international nor a regional financial center.

29. Nonetheless, the assessment team considers that certain features of various sectors in Estonia create significant ML/TF vulnerabilities associated, in particular, with the e-Residency program, CSPs and VASPs. These vulnerabilities generate major ML/TF risks, which have materiality that has not been duly acknowledged by the authorities through, *inter alia*, the NRA, the SRA and other strategic analysis products. In addition to the implications that these risks have within Estonia, they also have the potential of affecting risk profiles of other countries of the region and in wider geography. The paragraphs below reflect on the e-Residency program, CSPs

[47] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211220-1
[48] https://haldus.eestipank.ee/sites/default/files/2021-07/FSR_2021_eng.pdf, page 6
[49] https://www.imf.org/external/pubs/ft/wp/2007/wp0787.pdf;
https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm
[50] https://www.fsb.org/
[51] Finance Estonia (http://financeestonia.eu/about-us/) is a public-private financial sector cluster organisation with around a hundred companies and co-operative partners gathered under one roof.
[52] https://www.tallinn.ee/eng/clustersinestonia/financeEstonia
[53] The Effectiveness Questionnaire refers to the MERs of Isle of Man, Latvia, Switzerland, and New Zealand.

and VASPs as elements contributing to Estonia's risk and context with implications for a number of IOs/ themes in this MER.

30. The ***e-Residency program*** has been launched in 2014 to provide foreign citizens with access to Estonia's business environment and infrastructure through the e-Resident's digital ID issued by the Government[54]. The total number of digital ID's since the inception of the program has been around 92 thousand issued to nationals of more than 170 countries[55], of which around 58 thousand are valid as of April 2022. As of the end of 2021, e-Residents had established around 21.9 thousand companies in Estonia (8% of all companies), and the authorities advised that among economically active companies around 4.6 thousand (3% of all active companies) were connected to e-Residents[56]. In 2020, the Parliament's National Audit Office examined effectiveness of the program and identified a number of gaps in its functioning related to, *inter alia*, deficient control systems and failures to revoke digital ID of some e-Residents who committed a crime in Estonia or received a business ban abroad. Moreover, as further elaborated in IO.1, the assessment team has identified further gaps in the procedures of the competent authorities responsible for decisions related to e-Residency, mostly related to their inability of obtaining reliable and up-to-date information on the identity, criminal background, personal and business affiliations and other critical data on applicants from countries, with which Estonia does not have cooperation relations in the field of justice, security, or law enforcement[57]. At that, the program has had a large and increasing number of beneficiaries from jurisdictions in the FATF's black and grey lists[58], including two e-Residents from North Korea and one company established by them as of January 2022[59].

31. While the AT has not been provided reasonable explanation as to why tens of thousands of foreigners, especially those from EU and EEA, would need to spend time and money for obtaining digital identity in Estonia, there is information about involvement of e-Residents and companies established by them in various types of offences, including tax evasion[60] through, *inter alia*, VASPs licensed in Estonia. This is confirmed by the increasing number of international requests (both intelligence and MLA) involving subjects that are e-Residents or companies connected to them. Accordingly, the assessment team considers that the e-Residency program, while creating an Estonian and, in a broader sense, a European digital identity for a vast number of foreign

[54] The authority in charge of considering e-Residency applications is the PBGB, which cooperates with other competent authorities, including the ISS, the ETCB and the EFIU, to make decisions on issuance, renewal, suspension and revocation of digital IDs.
[55] The top e-Residency card holders are from Russia, Finland, Germany, Ukraine, China, the UK and France.
[56] https://www.stat.ee/en/avasta-statistikat/valdkonnad/majandus/economic-units
[57] At that, PBGB cases of sending international inquiries to foreign counterparts for more information on the applicants are rare (less than 10 per year), just as the cases of receiving feedback from domestic counterparts are (25-30 hints from the ISS and less than 10 from the EFIU annually against an average 12 thousand applications per annum).
[58] As of April 2022, the program has 873 beneficiaries (which established 288 companies) from jurisdictions in the FATF's black list; 6163 beneficiaries (which established 1684 companies) from jurisdictions in the FATF's grey list; and 1249 beneficiaries (which established 264 companies) from Estonia's own list of higher-risk countries (Algeria, Egypt, Saudi Arabia and Uzbekistan).
[59] As of May 2022, the website indicates one North Korean e-Resident and one company only, while as of July 2022 there is no indication of e-Residents or companies linked to North Korea. Nonetheless, in a separate file providing statistical information on non-resident beneficial owners of Estonian companies as reported to the Database of Beneficial Owners as of July 2022, there are still two individuals from North Korea identified as unique BOs of Estonian companies.
[60] See, for example, the analytical report published by the Finnish Tax Administration exploring whether Estonian companies connected to Finland or to Finnish nationals pose a significant risk in terms of the shadow economy (https://www.vero.fi/en/grey-economy-crime/scope/studies-on-the-shadow-economy/).

nationals, comprises a material vulnerability in the AML/CFT system of Estonia in providing beneficiaries of the program access to the business environment and infrastructure in Estonia, as well as in the countries where such identity is accepted. Such vulnerability is due to the fact that, especially in case of foreign nationals from third countries, the Estonian state does not know, to a sufficient extent of confidence, who the e-Residents are and to whom it has issued the Estonian digital identity, while in the narrower AML/CFT perspective it is not fully aware of the ML/TF and other threats emanating from the holders of digital identity. Moreover, the ML/TF risks emanating from this vulnerability have the potential of affecting risk profiles of other countries of the region and in wider geography in as much as the Estonian digital ID provides foreign economic operators and other decision makers an additional layer of confidence to consider the holders of such ID as individuals subjected to proper scrutiny by the Estonian state.

32. There is a significant sector of both ***licensed and unlicensed CSPs*** in Estonia. According to the analysis of ML risks of CSPs conducted by the EFIU in 2021[61], as of the end of 2020 there are 311 licenced CSPs in Estonia, along with a significant number of unlicensed CSPs, both legal entities and individuals factually providing such services, often connected with e-Residents. It remains unknown if, and to what extent, Estonian CSPs offer their clients trustee services on the basis of foreign law. Establishing and selling shelf companies is practiced among licensed and non-licensed CSPs (including the so-called multi-service providers). As of December 2020 approximately 10% of Estonian commercial entities and NPOs (26,349 legal entities) have been registered to 96 addresses and are often characterized by numerous indicators of shell enterprises (e.g. nominal directors, lack of employees and declared turnover, and failure to submit annual reports for several consecutive years). According to the EFIU analysis, some CSPs offer packages that also include presentation of fictitious beneficial owner data to the Business Register (BR). A large proportion of the service providers are incapable of effectively evaluating and detecting risks present in the sector, their awareness in AML/CFT matters is on average low, risk management systems are incomplete, measures of due diligence are insufficiently applied, and the obligation of reporting STRs is fulfilled only by very few service providers. International requests for information received by the EFIU indicate that the trend to use Estonian companies as shell companies has continued and even intensified.

33. Overall, the EFIU's analysis of CSPs confirms that Estonia as a jurisdiction is quite vulnerable in regard to corporate transparency and misuse of legal persons for criminal purposes. There are many indicators that Estonian companies are used as shell companies in international crime. The market for corporate services in Estonia is very active and a part of the services are clearly targeted at the international market. The assessment team considers that the features of the CSP sector described above make it a material vulnerability in the AML/CFT system of Estonia significantly deteriorating the quality of basic and beneficial information in the BR and creating additional opportunities for perpetrators to infiltrate the country's business environment and infrastructure. Moreover, ML/TF risks emanating from such vulnerability have the potential of affecting risk profiles of other countries of the region and in wider geography in as much as foreign economic operators and other decision makers perceive companies incorporated in Estonia as meriting of transparent basic and beneficial ownership.

[61] https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#money-laundering-ris

34. Estonia has been among the first countries to issue licences for ***VASP activity*** since the end of 2017, and the country positions itself globally at the forefront of crypto regulation. Due to the explosive growth of VASPs registered and licenced in Estonia, by the end of 2019 there were 2447 licenses issued by the EFIU. The authorities advise that after mass revocation in 2020 there were still around 400 valid VASP licenses[62] as of the end of 2021 for the provision of the whole range of relevant services. The licence issued by the EFIU is internationally advertised by Estonian CSPs as a quality sign to the VASP to confirm the clients that their property is in secure hands. The EFIU conducted two assessments of ML risks of VASPs through questionnaires sent to the market participants. Findings of these assessments were published in 2020 and 2022[63]. According to the findings of the most recent EFIU analysis, virtual asset services are concentrated in the hands of a few large service providers. The majority of VASPs does not have a payment account in an Estonian credit or payment institution and are serviced by foreign (e.g. Lithuanian and UK) payment and e-money institutions. Over 80% of the VASPs licensed by Estonia have only one Estonian person, either an individual or a legal entity, among the valid associations in the BR (shareholders, members of the management board and supervisory board, beneficial owners). Nearly 75% of Estonian VASPs have a CSP among associated persons. CSPs also offer VASPs the service of a nominal board member and shareholder (some law firms advertise the offering of such illegal nominal persons publicly on their websites). The VASPs licensed by Estonia predominately have 1-2 employees or no employees at all in Estonia, including those service providers with a turnover of hundreds of millions of euros.

35. The authorities admit that it is more complicated or practically impossible to execute supervisory proceedings in cases where the service provider is merely formally connected with Estonia. According to the findings of EFIU supervision, the level of application of due diligence measures of the majority of market participants is insufficient, and most VASPs lack effective surveillance and monitoring systems. The number of foreign requests received by the EFIU and the PBGB related to VASPs licensed by Estonia has been steadily increasing. The lack of reliable information on basic and beneficial owners, as well as managers of VASPs due to, *inter alia*, vast involvement of CSPs, extreme difficulty or practical impossibility of validating quantitative and qualitative indicators of VASP activity, as well as the lack of supervisory resources of the EFIU make Estonian VASPs a material vulnerability in the AML/CFT system of Estonia. Moreover, ML/TF risks emanating from such vulnerability have the potential of affecting risk profiles of other countries of the region and in wider geography in as much as the Estonian VASP license provides foreign economic operators and other decision makers an additional layer of confidence to consider such VASPs as entities subject to appropriate supervision for compliance with AML/CFT requirements.

1.3. Structural elements

36. Estonia has all of the key structural elements required for an effective AML/CFT system including political and institutional stability, governmental accountability, rule of law, and a

[62] Overall, information provided by the authorities on the total number of issued and revoked VASP licenses since the inception of the licensing regime is inconsistent and does not enable reliable conclusions on the number of valid licenses as of the time of the on-site visit.
[63] https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#money-laundering-ris

professional and independent legal profession and judiciary. It has a high level of commitment to dealing with AML/CFT issues.

37. The level of perceived judicial independence continues to be high[64]. There are nevertheless some weaknesses in the judicial system, particularly in terms of restricted understanding of ML, driven by the Supreme Court rulings, and undue delays in the criminal court proceedings. International reports do not point out integrity issues in the judiciary and the police.

1.4. Background and Other Contextual Factors

38. Estonia has an increasingly mature AML/CFT system, albeit there is room for some improvement. Since the last evaluation of the country in 2014, Estonia has initiated important changes in its AML/CFT Law on two occasions (this does not take account a number of interim revisions of the legislation), transposing into domestic framework Directive (EU) 2015/849 (the so–called 4th AML Directive) in 2017 and Directive (EU) 2018/843 (the so–called 5th AML Directive) in 2020. This allowed Estonia to follow global AML/CFT framework developments, expanding the domestic AML/CFT preventative system.

39. Financial exclusion is not an issue in Estonia. As one of the most advanced digital societies Estonia makes available for about 98% of inhabitants dispose of a bank account[65].

40. The GRECO evaluation report on Estonia (fifth evaluation round – Preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies) adopted in March 2021[66] does not suggest corruption is a major issue affecting Estonia. In Transparency International's 2021 Corruption Perceptions Index, Estonia scores 74 (out of a total score of 100), placing it at 13 out of the 180 countries included in the survey[67].

1.4.1. AML/CFT strategy

41. The AML/CFT Committee endorsed the Action Plan for combating ML/TF on 5 July 2021, which is considered to be the key strategic document aimed at mitigating risks/ addressing gaps in country's AML/CFT system. Building on the conclusions of the NRA 2021 report, the Action Plan sets 47 goals to be achieved in relation to an identical number of issues identified by the NRA, through activities with implementation deadline within 3-4 years (starting from the second half of 2021 until the end of 2024). The activities concern four domains (legislative, policy-making, implementation, and international cooperation) and are categorized by priority (very high, high, average, and low). Implementation of the activities under the Action Plan is distributed among ministries, supervisory authorities and agencies, specifying the lead authority responsible for the activity, and the partner authorities, which share responsibility for certain activities. AML/CFT Committee oversees implementation of the Action Plan.

42. Among national strategies and policies relevant for combating ML/TF, the authorities refer to the Strategy "Estonia 2035", the Fundamentals of Criminal Policy 2030, the Internal Security

[64] EU Commission, 2022 Rule of Law Report, p.3
[65] G20 Financial Inclusion Indicators | Estonia | The World Bank, https://www.afi-global.org/about/
[66] https://www.coe.int/en/web/greco/evaluations/estonia
[67] (the highest a country is positioned in the ranking, the least it is perceived as corrupt) https://www.transparency.org/en/countries/estonia

Strategy 2020-2030, the Foundations of Security Policy of Estonia, the Anti-Corruption Strategy 2025, the Priorities in the Fight Against Crime, the Strategy of the PBGB until 2030, the Strategy of the EFIU for 2022–2026, and the EFSA Operating Strategy for 2019-2021, which, to a varying level of focus and detail, define strategic goals, such as improving competence to fight serious covert crimes, preventing corruption and economic (including ML) crime, enhancing identification and confiscation of criminal proceeds, strengthening capacity to identify terrorist risks, raising awareness of ML/TF risks, and implementing risk-based supervision towards further improvement of the AML/CFT system in the country. Some of these policies and strategies have had relevant predecessors for earlier periods, as well.

1.4.2. Legal & institutional framework

43. The Money Laundering and Terrorist Financing Prevention Act (MLTFPA) is the central piece of legislation on AML/CFT matters. It requires the application of preventive measures, including STR reporting, by obliged entities, (including virtual currency service providers since 2017), the conduct of AML/CFT supervision by relevant authorities, and establishes sanctions. It also provides for the establishment and functioning of the EFIU and the approach for supervision, which is divided between EFIU, EFSA, Chamber of Notaries and Bar Association.

44. Other relevant pieces of legislation include the sectorial laws regulating the financial and DNFBP sector, the Penal Code (PC), the Code of Criminal Procedure (CCP), International Sanctions Act (ISA), and other sectorial legislation.

45. The institutional framework involves a broad range of authorities. The most relevant are the following:

46. The **AML/CFT Governmental Committee** is the primary mechanism for AML/CFT cooperation and coordination at the national level. It is a governmental committee with functions to coordinate NRA, monitor implementation of the Action Plan, develop AML/CFT policies and propose legislative amendments, pursue national cooperation in AML/CFT and in countering proliferation.

47. The AML/CFT Governmental Committee is organised by Ministry of Finance. The members of the committee are high level representatives of competent authorities: the Secretary General of the Ministry of Justice, the Secretary General of the Ministry of Interior, the Undersecretary for Financial Policy and Foreign Relations of the Ministry of Finance, the Undersecretary for Political Affairs of the Ministry of Foreign Affairs, the Head of the FIU, the member of the Management Board of the Financial Supervision Authority, the Undersecretary of Communications and State Information Systems of the Ministry of Economic Affairs and Communications, the Director General of the Police and Border Guard Board, the Prosecutor General, the Director General of the Tax and Customs Board, the Director General of the Internal Security Service, and the Deputy Governor of Eesti Pank.

48. **Estonian Ministry of Finance (MoF)** is responsible for the implementation of tax, financial and fiscal policies, and setting economic goals. It is also responsible for general policy, legislation and coordination of the activities in this area on AML/CFT.

49. **Ministry of Justice (MoJ)** is responsible for planning and carrying out the legal and criminal policy of the state, including by coordinating, together with other institutions fight

against crime and ensuring the security on the population. The Ministry is responsible for MLA, organisation and supervision of notarial services, oversight of the court registers, including the BR. The institutions under the MoJ administrat include also: (i) county, administrative and circuit courts; (ii) Prosecutor's Office; (iii) prisons; (iv) Centre of Registers and Information Systems; (v) Data Protection Inspectorate; and (vi)Estonian Forensic Institute.

50. **The Ministry of the Interior (MoI)** is responsible for implementation of activities related to the internal security of the state, public order, planning and coordination of development, and drafting of relevant legislation. Agencies under MoI dealing with ML criminal investigations are Police and Border Guard Board and Internal Security Service.

51. **Ministry of Foreign Affairs (MFA)** is responsible for coordination of the national implementation of international sanctions and represents Estonia in the respective international organisations.

52. **Estonian Financial Intelligence Unit (EFIU)** is the national centre for receipt analysis and dissemination of reports to national LEAs and foreign counterparts. The EFIU also carries out licensing of some sectors of OEs and supervision for implementation of AML/CFT requirements (see Table N°1.3).

53. The EFIU was a structural unit of the Estonian Police and Border Guard Board until 31 December 2020. Starting from 01 January 2021, the EFIU was established as a legal successor of the structural unit of Police and Border Guard Board, and became an administrative-type FIU, turning into a government agency under the jurisdiction of the Ministry of Finance.

54. **Estonian Financial Supervision Authority** (**EFSA**) exercises supervision over compliance with the MLTFPA, and legislation adopted on the basis thereof by credit institutions and financial institutions that are subject to its supervision under the Financial Supervision Authority Act and in accordance with the legislation of the European Union.

55. **Police and Border Guard Board (PBGB)** is the main competent authority for investigation of ML (unless the main offence is under the investigative jurisdiction of the ISS or the ETBC).

56. **Estonian Tax and Customs Board (ETCB)** is an investigative and surveillance authority which deals with the tax and border-crossing related crime. It investigates also ML when the predicated is a domestic tax crime. In addition, carries out administrative functions related to tax declarations and collection, and is responsible for licensing of organisers of gambling (games of chance, lottery games, casino games, betting games, slot–machine gaming, games of chance via Internet, telephone or other interactive communication means (online gaming).

57. **Internal Security Service (ISS)** is a body responsible for detecting, preventing and suppressing terrorism and TF and PF. ISS as a LEA is also tasked with detection and investigation of high level corruption, terrorism, proliferation of weapons of mass destruction, TF and PF.

58. **Prosecutor's Office (PO)** is in charge of pre-trial proceedings in Estonia and represent the state prosecution. The PO is divided into four district prosecutor's offices (Northern, Southern, Eastern and Western) and a central agency (Office of the Prosecutor General). The Office of the Prosecutor General (OPG) has two departments: the Supervision Department and the Prosecution Department. The ML and TF cases are led by prosecutors from the OPG and, also from the Northern District PO.

59. **Chamber of Notaries (CN)** is a self-regulatory body for Notaries. It conducts supervision over compliance with the requirements of the MLTFPA and legislation established on the basis thereof by notaries is performed by the MoJ, which has delegated supervision to the CN. The MoJ has retained the right to exercise administrative supervision. Administrative supervision verifies compliance with due diligence measures to prevent ML/TF, as well as compliance with other requirements related to the professional activities of notaries.

60. **Bar Association (BA)** is a self-regulatory body for attorneys-at-law, senior assistants of attorney-at-law and assistants of attorney-at-law. The BA supervises the professional activities and the performance of requirements of professional ethics of the members of the association and foreign attorneys operating in Estonia. Supervision is exercised by the board of the BA and disciplinary matters of attorneys are discussed by the court of honour of the association. This includes supervision of implementation of AML/CFT measures.

1.4.3. Financial sector, DNFBPs and VASPs

61. An overview of the financial and non-financial sector is provided in the table below.

Table N°1.1: Number of private sector obliged entities in Estonia

Obliged entities	Number (31.12.2021)	Size of sector EUR (31.12.2021)
FINANCIAL SECTOR		
Banks	15[68]	37 915 869 712 / assets
Payment service providers (PSPs)[69]	17	96 505 009 /assets[70]
Electronic money institutions	2	71 250 633 / assets
Consumer credit providers	68	4 271 059 436 / assets
Lending entities for legal persons	7	1 846 002 / assets
Leasing companies for legal persons	16	7 919 245/ assets
Investment firms	7	120 197 027 / assets
Money broking service providers	10	196 892 / turnover
Fund management companies	16	102 386 821 / assets
Small fund managers	56	551 318 415 / assets
Life insurance companies	5	2 503 962 164 / assets
Currency exchange offices	32	3 174 000 / turnover
Savings and loan associations	11	25 197 076 / assets
Guarantees and commitments service providers	3	93 057 / turnover
NON-FINANCIAL SECTOR		
Company service providers (CSPs)	325	62 630 141 / turnover
Casinos	26, of 3 land-based	25 997 345 / turnover
Entities engaged in trade of precious metals and stones (DPMS)	102	55 278 225 / turnover
Pawnshops	113	4 469 173 / turnover
Real estate brokers	191	40 567 917/ turnover
Notaries	88	39 561 396 / turnover

[68] Including 6 Branches
[69] Including 1 state owned UPSP providing internal money remittance services
[70] 343.2 mil EUR – value of the mediated services in 2020

Auditors (sole practitioner or partner/employee of audit firm)	346	34 072 854 / turnover
Certified accountants and tax consultants	6448	449 913 350 / turnover
Lawyers	859[71]	88 826 177 / turnover
VASPs		
VASPs	381[72]	20.3 billon[73]/ mediated services

62. The ranking of regulated sectors is based on their relative importance, materiality and the level of the risk in the context of Estonia. These rankings have been used to weight positive and negative implementation issues throughout the report, as a basis for conclusions.

63. **Banking sector** and **VASPs sector** are weighted as the most important in the Estonian context, based on their materiality and risk exposure.

64. The financial sector is dominated (around 80% of the total assets) by 15 **banks,** 6 of which are operating as branches of foreign credit institutions, with total assets of EUR 37.92 billion equivalent to 164% of Estonian GDP[74] in 2021. The foreign capital holds appr 90% of banking sector assets (including 57% - owners from Scandinavia and 24.4% - from USA). The Estonian banking sector is highly concentrated, with the four largest banks holding 90% of the banking assets[75]. Beside its size, the importance of the sector is also determined by the identification of serious AML/CFT breaches which led to closing the operations of a branch (2019) and initiation of a related criminal investigation (2017) and a licence withdrawal of a bank (2018). Likewise, as result of the recently identified serious AML/CFT breaches, criminal investigation was initiated in relation to one bank (2019). In terms of ML/TF risks, considering the cross-border profile of the criminal schemes in Estonia[76], banks are mediating around EUR 132 billion in cross-border payments (2020) (companies and financial institutions).[77] In the fourth quarter of 2021, cross-border payments constituted 41% of all payments made.[78] There is also a growth[79] in turnover and number of cross-border payments connected to customers of financial institutions and VASPs who are served by banks. This is particularly important in the context of the identified risk[80] in relation to the provision of payment services within the framework of correspondence relationships to clients who are financial institutions and VASPs (especially foreign VASPs) and are using current accounts or fund products to serve their clients.

65. Estonia was among the first jurisdictions to implement a regulatory regime for virtual assets in 2017, which made the country attractive for **VASPs** seeking a regulated status and led to a rapid growth of granted licences (2447 licences issued to 1308 unique virtual assets service providers by the end of 2019). This brought an increased cybercrime, fraud and ML/TF risks and,

---

[71] Out of the total 1074 members of the BA, 215 had suspended their membership.
[72] 369, as of 02 of May 2022
[73] Between July 2020 and July 2021
[74] https://haldus.eestipank.ee/sites/default/files/2021-07/FSR_2021_eng.pdf, page 6
[75] https://thebanks.eu/articles/banks-in-Estonia
[76] In 2021, the IMF was engaged by the Nordic-Baltic countries to conduct an analysis of cross-border ML/TF risks in the region, see: https://www.eestipank.ee/en/press/nordic-baltic-countries-engage-imf-conduct-analysis-cross-border-money-laundering-and-terrorist-21012021
[77] Sectoral ML/TF risk assessment of the financial sector (May 2021), page 7
[78] https://www.eestipank.ee/en/press/statistical-release-turnover-cross-border-payments-increased-substantially-fourth-quarter-26012022
[79] Sectoral ML/TF risk assessment of the financial sector (May 2021), page 30
[80] Sectoral ML/TF risk assessment of the financial sector (May 2021), page 5

as evidenced by the LEAs, using virtual currencies in criminal schemes became common in Estonia.[81] The efforts of the authorities initiated in 2020 to strengthen the regulatory regime and de-risk the sector resulted in revocation of roughly 70% of the licenses (according to the information provided by the authorities, as of the end of 2021 there were 381 valid licences and 252 active VASPs). Despite the decreasing number of market participants, the value of the mediated services by the remaining VASPs increased nearly eight times from July 2020 to July 2021[82] and the number of clients has increased nearly 4.5 times compared to 2019 (4.8 million clients, of which 2 million are active)[83]. The Estonian VASP sector is considered to be concentrated, as more than 85% of the total turnover (EUR 20.3 billion: July 2020 - July 2021) was generated by 15 VASPs. The NRA identifies VASPs as high risk for ML and TF, which also corresponds with the perception of the private sector. As a result, the vast majority of the Estonian VASPs do not have a payment account in an Estonian payment or credit institution and are serviced by foreign payment or e-money institutions. As indicated by the SRAs of the VASP sector of 2020 and 2022, the use of Estonian VASPs for laundering the proceeds of fraud, ransom, drug crime etc. has been confirmed by the received foreign requests and by the Estonian criminal proceedings. The importance of the sector is also accentuated by the general low level of due diligence measures, which is significantly insufficient compared to the specific risks and the volume of services offered, lack of efficient monitoring systems and a low level of reporting

66. **Investment firms:** is weighed as important in the context of Estonia. The overall ML/TF risk attributed by the NRA 2021 to the financial sector is "average". The 2021 EFSA Sectoral risk assessment of the financial institutions highlights the investment firm sector as the second sector, after banks, that is exposed to the cross-border threat, considering the number of non-resident clients and the volume of provided services. The value of the client assets managed in 2020 was around EUR 403 million, or 1.5% of GDP[84] . During 2016-2020, between 94%-99% of the assets under management were owned by non-residents, the majority of whom are from Russia.[85]

67. **MVTS:** is weighted as moderately important in the Estonian context. The sector is represented by the non-bank payment service providers (PSPs) and e-money institutions (EMIs). The most common payment services in Estonia are money transfers, card payment processing, and initiation of payments from an account or with a card. The sector is highly concentrated, as the three largest of the providers had 97% of the whole market turnover of payments in 2020. The share of the payment transactions made in 2020 by the payment service providers of all payment transactions is rather small, namely less than 2%, with a focus on serving Estonian residents[86]. Nevertheless, in 2021 the size of the sector has increased substantially comprising 16 payment service providers and two e-money institutions with a total value of assets of EUR 167.7 million. The value of the assets in 2020 was two times lower (EUR 81.4 million). This is due to the new market entrants – 3 PSPs and 2 EMIs (which became operational). The exposure of the sector to the cross-border ML/TF varies, depending on the value of the cross-border payments made. While in 2020 the value was around 17.7 million per quarter, in the previous year (2019)

[81] Sectoral Risk Assessment of VASPs (2020), page 22, §3.3
[82] Sectoral Risk Assessment of VASPs (January 2022), page 3
[83] Sectoral Risk Assessment of VASPs (January 2022), page 4
[84] The Structure of the Estonian Financial Sector, 2021, page 19
[85] Sectoral ML/TF risk assessment of the financial sector (May 2021), page 37
[86] Sectoral ML/TF risk assessment of the financial sector (May 2021), page 38

the value was more than five times higher, with EUR 97.3 million per quarter. There is no available information on the value of the payments made by the MTVS sector related to cross-border threats in 2021. Nevertheless, it is expected to be higher considering that in the fourth quarter of 2021, the total turnover of cross-border payments increased substantially (up to 90.9% on the same period a year earlier).[87]

68. **Fund managers:** is weighted as moderately important in the Estonian context due the recent significant increase of the size of the sector. The value of the assets in 2021 was EUR 653.7 million, which is around five times higher than in the previous year. Likewise, the number of the market participants has increased in relation to small fund managers (56 in 2021, compared to 23 in 2020). The factors which led to such development of the sector remain unknown. The sector was assessed in 2021 as posing a rather low ML/TF threat, mainly due to the fact that the vast majority of the assets managed were related to mandatory pension funds which are financed from the official salaries. Nevertheless, in circumstances where the assets of small fund managers (not related to the management of mandatory pension funds) exceed five times the value of the assets of the fund management companies, this conclusion is no longer relevant.

69. **Life insurance companies** and **consumer credit providers** are rated as less important in the context of Estonia, as the sectors are highly concentrated, most of the assets/ market share are hold by companies part of banking groups, the focus of the services on resident natural persons, and very small average balance of consumer credit agreements.

70. Other FIs, such as lending and leasing companies providing services for legal persons, money broking service providers, savings and loans associations, guarantees and commitments service providers and currency exchange offices, are weighed as being of relatively low importance in Estonia's context based on their materiality and risk.

71. **CSPs:** is weighted as the most important DNFPB sector in the context of Estonia. The NRA 2021 identifies an average ML/TF risk in relation to the CSPs sector, an average-high score in terms of the supervisory priorities and concludes on the need to improve the incomplete overview of the sector. The more recent analysis[88] of ML risks of CSPs conducted by EFIU in 2021 highlights a series of vulnerabilities and features of the sector which indicate a significantly higher ML risk. There is a substantial number of unlicensed CSPs. Forty percent of the companies that factually have characteristics of providing corporate services operate without a valid licence. About 19% of the 311 licensed CSPs do not have the characteristics of factual service providers and are often connected with e-residents (more than half of them originating from third countries). It remains unknown if and to what extent the Estonian CSPs offer their clients the service of trust, on the basis of legislation of some country that recognises trust[89]. The sector is known for its high-risk appetite (e.g., establishing and selling shelf companies, large number of established VASPs which were sold to e-residents and non-residents), which is not counterbalanced by appropriate mitigation measures. The NRA 2021 identifies a low level of awareness and application of the AML/CFT obligations across the sector.

[87] Turnover of cross-border payments 2021
[88] https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#money-laundering-ris
[89] As Estonia does not recognise trusts nor other arrangements according to the law.

72. **Real estate brokers and notaries** are weighed as important in the context of Estonia, due to the risk and cases[90] of real estate investments coming from third countries using money of suspicious origin, including virtual currency. The importance is also substantiated by the recent significant growth of the sector (with 61.5% in 2021, compared to 2020) and the sectoral vulnerabilities, such as the lack of licencing and qualification requirements for the real estate agents, low awareness of the AML/CFT obligations and relatively weak supervision. The Action Plan based on the NRA 2021 identifies the actions for addressing the vulnerabilities of the real estate sector as high priority. Notaries play a significant role in real estate deals due the requirement of mandatory notarial authentication. In 2019, 66% of the STRs submitted by notaries in 2019 concerned real estate transactions in total amount of approx. 60.62 million euros.

73. **DPMSs:** is weighted as moderately important in the Estonian context due to its materiality, the level of ML/TF risks exposure and the vulnerabilities of the sector. DMPS is regulated for AML/CFT purposes when cash payments exceed EUR 10 000 and certain activities, such as buying-in or wholesale of precious metals and/or precious metals articles used for production, scientific and/or medical purposed, are excluded from the AML/CFT obligations. The NRA 2021 conclusions on the "below average" ML/TF risk refer to dealers' sector, comprising a wide range of market representatives (including construction, vehicles, retail sales, real estate, luxury goods, healthcare, transport) and not specifically to the DPMS sector. The low threat of cash transactions was assessed based on the frequency of cash withdrawals from ATMs[91] and the survey responses (58.5% of the respondents indicated cash transactions and 3% - cash transactions above EUR 10 000). However, the response rate received from DPMSs was the lowest among the inquired market representatives (45%). The geographical position of Estonia increases the risks for the sector of being misused[92]. The sector has a low awareness of the AML/CFT requirements, including the duty to report, the obligation to perform more substantive background checks on customers and on third parties participating in transactions, and the obligation to identify politically exposed persons (PEPs) and its supervision is relatively weak.

74. **Casinos:** is weighted as moderately important in the context of Estonia, due to the materiality of the sector among other DNFBPSs, the large amount of money moved through the gambling sector, a considerable part being cash, the insufficient awareness of the AML/CFT obligations, including low number of STRs and other type of reports (apart from one active market participant), the relatively weak supervision of the sector and the cases of suspicions of involvement in illegal activities such as fraud and ML[93].

75. Other DNFBPs, such as lawyers, auditors, accountants and tax consultants, are weighted as being of relatively low importance in Estonia's context based on their materiality and risks, including based on the conclusions of the 2020 NRA which indicates a below-average ML/TF risk regarding liberal professions.

[90] Analytical reports of PBGB (2020 and 2021); NRA 2020, Chapter 3, page 7
[91] The value of cash withdrawals indicated in 2021 an average of EUR 10.2 million per day: Statistics eestipank 2021
[92] NRA 2020, Chapter 9, page 10
[93] Analytical reports of PBGB (2019).

1.4.4. Preventive measures

76. The preventive measures are set out in the MLTFPA and accompanied by sectoral guidelines. The previous MLTFPA that had been in place since 2008 and at the time of the previous round of assessment of Estonia was ceased in 2017 with the adoption of the new MLTFPA, which has been revised and amended in 2019, 2020 and 2021. The changes and amendments introduced into the MLTPFA were initially driven by the implementation of the 4th and 5th EU AMLD, and meeting recommendations made in the 4th round of MONEYVAL assessment, and advancements of the AML/CFT system in the country.

77. The current legislation provides for some exemptions from FATF Recommendations requiring DNFBPs to take certain actions. In particular, according to MLTFPA, competent supervisory authorities may, at the request of the obliged entity, except for those supervised by the EFSA, i.e. credit and financial institutions, decide that the preparation of a documented risk assessment[94] is not mandatory having regard to the NRA and where specific risks of the respective sector are clear and understandable, or where the risk assessment prepared by the supervisory authority or the NRA has established risks, risk appetite and risk management model of the respective sector, and the obliged entity implements these. The authorities advise that such exemption has been requested only once by auditors and declined by the EFIU.

78. In addition, according to MLTFPA the following categories of entities are excepted from the AML/CFT framework. Those are: (i) the persons engaged in buying-in or wholesale of precious metals and precious metal articles used for production, scientific or medical purposes; (ii) an insurance undertaking providing services related to mandatory funded pension insurance contracts within the meaning of the Funded Pensions Act; and (iii) a management company upon managing a mandatory pension fund within the meaning of the Funded Pensions Act, and an investment fund founded as a public limited company within the meaning of the Investment Funds Act. Those exceptions are not supported by substantive assessment of ML/TF risks concluding that there is a proven low risk in those sectors or activities, and that those exceptions occur in strictly limited and justified circumstances.

79. Estonia extends application of preventative measures to certain activities that are not covered by the FATF Standards i.e., undertakings providing a cross-border cash and securities transportation service; pawnbrokers; auditors, tax advisors, dealers in art objects, and the organisers of games of chance other than casinos (with the only exemption of promotional lotteries), non-profit organisations dealing with EUR 5000 cash sums and the Central Bank of Estonia, where it exchanges cash over 10 000 or sells collectors' coins over such value.

1.4.5. Legal persons and arrangements

80. The legal instruments regulating creation and types of legal persons include the General Part of the Civil Code Act (GPCCA), the COC, the Non-Profit Associations Act (NPAA) and the FA, as well as well as special laws on specific types of legal persons[95]. As described in detail in the technical compliance analysis for R.24, the COC defines five forms of business entities – general

[94] As required under FATF R.1, criterion 1.10 and MLTFPA Section 13(1).
[95] E.g. land improvement associations and apartment associations, whose purpose is not to seek profit, but to govern a part of land or a block of apartments (residential buildings).

partnerships, limited partnerships, public limited companies[96], private limited companies[97] and commercial associations, while the NPAA and the FA define two forms of non-business entities – non-profit associations and foundations. In addition, three types of European companies may be created in Estonia – European public limited liability companies[98], European cooperative societies[99] and European economic interest groupings[100]. The passive legal capacity of business and non-business entities commences as of their entry into, and terminates upon their deletion from, respectively, the CR and the Register of Non-Profit Associations and Foundations (NPAR).

81. The Registration Department of Tartu County Court is the processor of the CR and the NPAR (collectively called the BR, for which the controller is the MoJ) and, since 7 March 2022, of the Beneficial Ownership Information Database (BOID, for which the controller is the Ministry of Finance), in charge of all procedures specified in relevant legal acts. The Center of Registers and Information Systems (CRIS) is the other processor of all mentioned databases, providing the necessary IT infrastructure and technical support. CRIS maintains the web portal e-Business Register, which provides centralized and uniform access to all mentioned, as well as other databases (e.g. the Commercial Pledge Register, the Land Register, the Database of Trade Bans, as well as some fields from other databases containing information on, inter alia, amount of paid taxes, taxable turnover, tax arrears etc.).

82. The table below gives a general overview of the dynamics in creation of legal persons in Estonia over the last five years:

Table N°1.2: Total number of legal persons per type, as at end of year

Type of legal person	2017	2018	2018	2020	2021
General partnership	1367	1369	1965	1441	1398
Limited partnership	4287	4217	4605	6392[101]	6542
Public limited company	3189	3036	2933	2851	2769
Private limited company	174170	193311	201793	219207	241181
Commercial association	1714	1727	1708	1698	1690
Non-profit association	32928	31133	21892	22609	23337
Foundation	792	813	814	818	819
Land improvement association	0	0	3	37	65
European public limited liability company	7	11	12	12	12
European cooperative society	0	0	0	1	1
European economic interest grouping	19	19	19	19	19
Total	**218473**	**235636**	**235684**	**255085**	**277833**

[96] The minimum share capital of a public limited company is EUR 25 thousand.
[97] The minimal share capital of a private limited company is EUR 2.5 thousand.
[98] Abbreviated as SE, which may be formed by at least two existing companies originating in different EU countries.
[99] Abbreviated as SCE, which may be formed by five or more individuals or companies based in at least two countries with the EEA.
[100] Abbreviated as EEIG, which may be formed by companies or individuals in accordance with the laws of an EU country.
[101] The authorities advise that the sharp increase in the number of limited partnership was partially due to the change in the solar power production subsidies, whereby only small producers qualified, most of them established in the form of a limited partnership.

83. Estonia in not a party to the Hague Convention and does not recognise trusts nor other arrangements according to the law. However, trusts and similar legal arrangements set up under foreign laws may still carry out financial and other activities in Estonia, albeit by deploying a representative and under another country's legal provisions.

84. The authorities advise that they have engaged extensively with licenced CSPs and, in addition, have actively looked for actors that might provide company and trust services with no valid activity license (EFIU analysis of CSPs, 2021). In the course of these engagements the authorities have not obtained information that Estonian CSPs are engaged in the provision of trustee services, although they admit that their presence cannot be excluded

1.4.6. Supervisory arrangements

85. There are four supervisory authorities in Estonia – EFSA, EFIU, CN and BA.

86. The EFSA exercises supervises the majority of FIs, including credit institutions, life insurance companies, investment firms, fund management companies, payment service providers, e-money institutions and consumer credit loan providers as well as branches of the said institutions operating in Estonia through the freedom of establishment principles of European Union.

87. The EFSA acts as an AML supervisor, prudential supervisor and as a resolution authority.

88. The EFIU supervises FIs that are not supervised by the EFSA, including bureau de exchange, management companies and investment funds that do not meet the licensing obligation under the Investment Funds Act, guarantees and commitments service providers, money service businesses that do not fall under the Payment Services and E-money Services Act, borrowing and lending operations for legal persons, leasing operations for legal persons, savings and loan associations, provision of advice on financial services.

89. The EFIU also supervises DNFBPs (other than notaries and lawyers that are members of the bar), including casinos (including internet and ship-based casinos), CSPs, pawnshops, dealers in Precious Metals and Stones, other persons trading in goods, lawyers, auditors, notaries, bailiffs (enforcement agents in MLTFPA), bankruptcy trustees, accountants, tax Consultants, real estate brokers.

90. Lastly, the EFIU supervises VASPs, however there is a legislative intent to bring them under the supervision of the EFSA.

91. The CN supervises notaries.

92. The BA supervises lawyers that are member of the bar.

Table N°1.3: Supervision of FIs and VASPs

Type of FI and VASP	AML/CFT Supervisor	Licensing Body (Market Entry)
Banks	EFSA	EFSA
Life Insurance	EFSA	EFSA
Fund management	EFSA	EFSA
Investment Firms	EFSA	EFSA
PSPs	EFSA	EFSA
EMIs	EFSA	EFSA
Consumer credit providers	EFSA	EFSA

Currency Exchange Offices	EFIU	EFIU
Other financial institutions[102]		
Borrowing and lending operations for legal persons	EFIU	EFIU
Leasing operations for legal persons	EFIU	EFIU
Management companies and investment funds without activity license (small fund managers)	EFIU	EFIU
Money service businesses provided based on a brokerage contract (Art. 658 Law of Obligations Act)	EFIU	EFIU
UPSP (internal money remittance services)	EFIU	ECA[103]
Savings and Loan Associations	EFIU	EFIU
VASPs	EFIU*	EFIU*

* There is a legislative proposition to transfer the supervisory arrangements over VASPs from the EFIU to the EFSA.

Table N°1.4: Supervision of DNFBPs

Type of DNFBP	AML/CFT Supervisor	Licensing Body (Market Entry)
Casinos	EFIU	ETCB
TCPS	EFIU	EFIU
Pawnshops	EFIU	EFIU
DPMS	EFIU	EFIU
Lawyers	BA	BA
Notaries	CN	MoJ
Other independent legal professionals	EFIU	None
Auditors	EFIU	Auditing Activities Oversight Board
Accountants, Tax Consultants	EFIU	None
Real-estate brokers	EFIU	None

1.4.7. International cooperation

93. International cooperation is particularly important for Estonia, given its risk profile, geographical location, and the fact that the majority of criminal cases have an international component (ML, TF, fraud, drug trafficking, trafficking in human beings, etc.). Overall, Estonia has adequate mechanisms, including an extensive network of multilateral treaties, to provide and seek the broadest range of mutual legal assistance (MLA) and extradition in relation to ML, associated predicate offences and TF. This especially applies to cooperation with EU-member states. Most of the foreign cooperation is conducted via the dedicated mechanisms provided for the EU Member States (EIO and EAW). Estonia made the reservation to the European Convention on Mutual Assistance in Criminal Matters (ETS no. 030), reserving the right to refuse cooperation in a case when the request concerns an act that is not considered an offence under Estonian laws.

[102] Unlicensed by the EFSA

[103] Estonian Competition Authority

2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 1

a) The mechanism for nation-wide identification, assessment and, subsequently, understanding of ML/TF risks in Estonia involves national risk assessments coordinated by the AML/CFT Committee with high-level commitment and nationwide coverage, access to all data available in the country from public and non-public sources. This provides a sound basis for the authorities to build and develop the understanding of ML/TF risks facing the country.

b) Other strategic analysis products, such as the EFSA's SRA (2021), ORTO Project (2018-2019) and analysis of VASP-related services (2021), EFIU's analyses on CSPs (2021) and VASPs (2020 and 2022), international cooperation (2021 and 2022) and NPO risks (2022) certainly contribute to better understanding of risks in the respective sectors.

c) Nonetheless, nation-wide efforts underpinning the understanding of ML/TF risk do not provide for uninterrupted coverage of considered periods, timely endorsement and dissemination of relevant outcomes, which, in turn, do not reliably assess, and give a comprehensive view of, the (residual) ML/TF risks in the country. There are important missing elements in the current understanding of ML/TF threats and vulnerabilities.

d) The authorities develop and endorse action plans as nation-wide AML/CFT policies based on the findings of the NRAs. Nonetheless, current practices do not provide for uninterrupted availability of such policies, appropriate prioritisation of the measures set out in them, and proper attention to a number of higher risk areas and issues.

e) The part of the authorities' activities related to dealing with the multinational "laundromats" in the recent past has not had the required impact in due time, while the missing elements in the present understanding of the ML/TF risks do not provide for effective and timely response to existing and potential risks concerning, first of all, the e-Residency program, activities of CSPs and VASPs, and a special cluster of customers (VASPs, PSPs and EMIs).

f) National cooperation and coordination is a strong feature of the AML/CFT system in Estonia, supported by regular work of the high-level AML/CFT Committee, operational-level working groups/ platforms, as well as adequate bilateral cooperation mechanisms and practices. The framework for cooperation and coordination in the area of combating PF does not appear to be clearly defined and consistently implemented.

g) Unlike VASPs and most of the representatives of the DNFBPs, major players in the financial sector confirm participation in the most recent nation-wide risk

assessment, demonstrate awareness of its outcomes and elaborate on their integration into own enterprise-wide risk assessments.

Recommended Actions

Immediate Outcome 1

a) Estonia should take measures to significantly enhance the understanding of ML/TF risk faced by the country through, *inter alia*, improvement of nation-wide ML/TF risk assessments so as to provide for uninterrupted coverage of considered periods, timely endorsement and dissemination of relevant outcomes. Such outcomes should reliably assess ML/ TF threats and vulnerabilities and give a comprehensive view of the (residual) ML/TF risks in the country.

b) Estonia should take measures to significantly improve the practice of developing and endorsing nation-wide AML/CFT policies so as to provide for their uninterrupted availability, appropriate prioritisation of the measures set out in such policies, and proper attention to the higher risk areas and issues.

c) The current national AML/CFT policy (the Action Plan) should be revised in order to comprehensively address, as a matter of priority, the issues identified in relation to insufficient capacities and practices of competent authorities to identify, assess and mitigate ML/TF risks concerning the e-Residency program, the special cluster of customers (VASPs, PSPs and EMIs), as well as the activities of CSPs and VASPs.

d) Outcomes of nation-wide risk assessment exercises should be integrated into the objectives and activities of individual authorities so as to enable proactive, timely and decisive actions aimed at mitigating the existing risks, as well as preventing generation of new ones.

e) The framework for cooperation and coordination in the area of combating PF should be clearly defined and consistently implemented by means of, *inter alia*, delineating (or otherwise harmonizing) relevant mandates of the AML/CFT Committee, the SGC and the SCIIS, and providing for direct involvement of the EFIU in CPF matters.

f) Actions should be taken to improve awareness of DNFBPs and VASPs about outcomes of nation-wide risk assessments and their integration into own enterprise-wide risk assessments. The private sector should be provided with specific guidance on the implementation of the recommendations of the NRA.

94. The relevant Immediate Outcome (IO) considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1. Country's understanding of its ML/TF risks

95. The mechanism for nation-wide identification, assessment and, subsequently, understanding of ML/TF risks in Estonia involves national risk assessments coordinated by the AML/CFT Committee. The MLTFPA defines conduction of NRAs as a periodic exercise aimed at, *inter alia*, identifying the needs for improvement of AML/CFT legislation, specifying areas of higher and lower ML/TF risk, and guiding activities of competent authorities in allocation of resources and setting priorities for AML/CFT purposes. Due to high-level commitment and nationwide coverage, the NRA has access to all data available in the country from public and non-public sources. This provides a sound basis for the authorities to build and develop the understanding of ML/TF risks facing the country. So far, the authorities have conducted two NRAs – the first covering the period 2011-2013, with the report endorsed in January 2015 and published in March 2018, and the second covering the period 2017-2019, with the report endorsed in April 2021 and published in May 2021. Hence, the current approach and practice of conducting NRAs do not provide for uninterrupted coverage of considered periods, as well as timely endorsement and dissemination of the assessment outcomes.

96. On the threat side, the NRA 2021 identifies higher threats associated with VASPs, CSPs, foreign trade-related cash flows, activities of e-Residents and tax evasion. On the vulnerability side, the report highlights vulnerabilities related to VASPs, CSPs, application of confiscation measures in practice, performance of some supervisory authorities, criminal investigations connected to ML, including predicate offences, limited ability of strategic analysis, issues related to misdemeanours and low level of fines, insufficient national statistics, and lack of the reporting obligation for some sectors. Hence, while the NRA 2021 report provides useful hints on sectors with higher risk exposure, such as the VASPs and CSPs, its conclusions are set out in terms of prevalent threats and vulnerabilities assessed descriptively (high, above average, average, below average, and low) and numerically (on a scale of 1 to 5), which do not give a comprehensive view of the (residual) risks of ML and TF in the country. Moreover, for the reasons described in Chapter 1 and TC Annex (R.1) of this report, the conclusions of the NRA 2021 report do not appear to be a reliable assessment of ML/TF threats and vulnerabilities in Estonia, both in terms of descriptive estimates and numerical scores.

97. Other strategic analysis products, such as the EFSA's sectorial risk assessment (2021), EFIU's analyses on CSPs (2021), VASPs (2020 and 2022), international cooperation (2021 and 2022) and NPO risks (2022) certainly contribute to better understanding of risks in the respective sectors. Nonetheless, there are important missing elements in the identification, assessment and, consequently, understanding of ML/TF threats emanating from both registered and non-registered (undetected) domestic proceeds-generating crimes, organized crime, cross-border movement of funds and cash, ML/TF vulnerabilities in private and public sectors, risks related to the abuse of legal persons (including through the e-Residency program), activities of CSPs and VASPs, as well as the country's exposure to the risk of TF.

98. With regard to the assessment of national **ML/TF threats**, neither the NRA 2021 nor other strategic analysis products provide comprehensive analysis on ***domestic proceeds-generating crimes***, at least from the standpoint of their occurrence and the amounts involved, as well as the

damage ascertained through investigations, prosecutions and convictions. The SRA 2021 comprises a section[104], which provides statistics for 2019 on the number of criminal offences registered in the country. This is followed by subsections on various types of offences[105], where analysis, if any, is limited to the number of registered cases and the amount of incurred loss, supported by assumptions about the share of cases that could generate proceeds of crime for further laundering, as well as the potential non-registered (undetected) crimes with expert estimates of the possible amount of criminal proceeds. The analysis summarizes with a calculation of the estimated amount of domestic criminal proceeds, providing two almost equal figures – one within the rage of EUR 81 to 118 million and the other equal to EUR 103 million – using two alternative sources of information and two different sets of predicate offences[106]. Overall, this exercise seems to lack reliable source data, proper methodology and consistent analysis to produce reasonable outcomes.

99. The NRA 2021 acknowledges the presence of ***organised crime*** in Estonia whereby, in order to organize ML, both natural and legal persons are exploited through using their bank accounts for receiving and transferring money against a fee. It refers to examples of convicting perpetrators for, *inter alia*, formation of and membership in a criminal organization. The PBGB advises that since 2018 it regularly creates and annually updates national level OCG profiles, evaluating every OCG against 15 criteria[107]. It assures that active OCG's are currently paralysed due to successful work of the PBGB, particularly the efforts of the National Criminal Police (NCP) since 2014 targeting the heads of the most influential OCGs and thus creating a situation where their activity is hindered[108]. According to the authorities, organized crime is moving towards white-collar offending, particularly fraud and tax fraud, and the PBGB has mapped out OCG-related companies and assessed the tax evasion and ML risks in cooperation with the ETCB and the EFIU. This does not reconcile with the authorities' assessment of prevalent predicate offences in Estonia, where tax offences are the last among the four major proceeds-generating crimes according to the estimates based on the SRA 2021 data and are not identified as a prevalent crime according to the estimates based on the Statistical Office data.

100. Without challenging the achievements of competent Estonian authorities in the suppression of "traditional" organized criminality (grouped around leaders with obvious criminal background, whom the Estonian media describes as the "businessmen" in black leather jackets hiding their eyes behind black glasses), the assessment team considers that the above-mentioned

---

[104] Section 4.1, "The volume and structure of Estonian criminal proceeds and thus, the volume of predicate crimes, i.e., the threat of domestic money laundering".
[105] Such as theft, fraud and embezzlement, drug crimes, tax offences, corruption, and environmental offences.
[106] In particular, the first estimate using the data collected for the SRA 2021 and referring to the crimes of fraud, embezzlement, drug and tax offences concludes that the potential amount of domestic criminal proceeds is within the range of EUR 81 to 118 million per year. The second estimate using the data of the Statistical Office and referring to the crimes of alcohol, tobacco and fuel smuggling, prostitution and drug offences concludes that the domestic criminal proceeds potentially amount to EUR 103 million per annum.
[107] Such as field of crime, geographical ambition, infiltration to the legal businesses, different kinds of assets under control, ML risk etc.
[108] The authorities provided a link to the publication in the in 2019 Yearbook of the Prosecutor's Office, which refers to a statement made in 2018 by the Director General of the PBGB assuming that *"there are about 20 criminal associations in Estonia, we have mapped them and consider seven-eight-nine of them dangerous"*, describes some episodes related to the activities of once-powerful criminal organizations in Estonia since 1990s and to the successful imprisonment of some of their leaders, concluding that *"so far, organised crime in Estonia will be "headless""* and that *"it is too early to rest on the laurels"*.

statements and assurances do not amount to a comprehensive view of the OCG presence and significance in the criminal landscape of the country, both in terms of the most prevalent *modi operandi* used by criminal groups, and of reliable estimates regarding the proceeds of crime factually or potentially owned/controlled by them. At that, according to information from reliable public sources[109], the strategic location astride Eastern and Western Europe makes Estonia a targeted transit country for crime groups smuggling illicit merchandise between those markets. Consequently, the country's principal transnational crime challenges include trafficking in drugs, people, weapons as well as illegal migration, while associated crime include ML and violent crime.

101. The understanding of threats related to the ***cross-border movement of funds*** is limited to a conclusion of the NRA 2021 reading that *"it is not possible to assess threats or risks related to ML as pertaining to countries"*. The SRA 2021 comprises a section[110] with subsections considering cross-border payments, deposit and loan products offered by credit institutions, as well as services provided by other financial institutions. It points out that over the period 2013-2019 the ratio of foreign payments to GDP, as well as the ratio of foreign payments to international trade (import and export) have significantly decreased from 7.5 and 4.1 in 2013 to, respectively, 4.2 and 2.8 in 2019. The report also analyses a number of statistical indicators to compare Estonia's position in terms of cross-border movements of funds with that of other EU Member States. Nevertheless, this means that as of the end of 2020 there is still a high level of cross-border transactional activity mediated by banks annually in the financial sector with around EUR 60 billion in credit (customer) transfers and around EUR 62 billion in payments between financial institutions, a very significant part of which is not demonstrably related to the creation of GDP in the economy, international trade or otherwise reasonably explained in terms of potential ML/TF risk exposure.

102. The knowledge on threats related to the ***cross-border movement of cash*** is limited to a conclusion of the NRA 2021 reading that *"it is not possible to identify threats or risks related to ML on the basis of cash flows alone"*, statistics on the numbers of requests sent and received by the EFIU, and statistics on the number and amount of cash declarations at the EU border. This is not supported by analysis and conclusions about the economic or other legitimate rationale and, subsequently, the potential of the mentioned cash movements in terms of facilitating possible ML or TF (e.g., consideration of the number of and amounts in declarations in terms of economic and other rationale in relations with the higher risk countries or destinations). The only explanation provided in this regard is that the total value of cross-border movements of cash is low compared to that of funds (e.g. in 2020 EUR 4.6 million incoming and EUR 7.5 million outgoing), and that most of cash movements is facilitated by one currency exchange service provider (fluctuating over years between 80-90% of total cross-border cash movements, as seen from the cash declarations and CTRs reported by the same entity). Cross-border movement of funds and cash are not considered in the context of the EIOs, MLAs and EFIU exchanges of information vis-à-vis underlying predicate offences and ML/TF trends or patterns. The ETCB advises of having implemented the Customs Compliance measurement system since 2011, which enables selection of control objects according to predefined rules in correlation with, *inter alia*, traffic intensity. Cash-related risk profiles (e.g., descriptions of cash concealment methods) are implemented into

[109] https://www.interpol.int/Who-we-are/Member-countries/Europe/ESTONIA
[110] Section 4.2, "Risk of money laundering from other countries i.e., cross-border money laundering threat".

the ETCB database and are obligatory for all customs officers. The potential occurrence and amount of undeclared cash smuggled through the border is reported to be low.

103. The assessment of national **ML/TF vulnerabilities** lacks proper analysis of a number of important elements. Particularly, in the NRA 2021 vulnerability due to ***the reporting duty and the application of preventive measures*** is assessed below average, with no analysis of the effectiveness of STR reporting (including consistency with prevalent ML/TF threats and typologies in the country), on the background of the lack of reporting and low level of compliance by the highest risk sectors of CSPs and VASPs. At that, performance characteristics of obliged entities, such as the efficiency of compliance control systems or quality of CDD measures, are assessed high judging upon their responses to the NRA questionnaire without relevant feeds from the outcomes of supervision. Moreover, vulnerability due to ***the capabilities of supervisory authorities*** is assessed low albeit the obvious resource constrains of the EFIU (at least at the time of conducting the NRA), with little or no analysis of the capacities of sectorial supervisors (such as the BA and the CN), and the effect of complexities in addressing infringements of AML/CFT obligations through misdemeanour proceedings. Then, vulnerability due to ***the restrictive interpretation of the ML offence set by the Supreme Court rulings*** is also assessed as low (see the analysis under IO.7 for further details). Such estimate of the vulnerability is not supported by analysis on the outcomes of ML/TF investigations, prosecutions, convictions and confiscations to demonstrate effectiveness of the respective stakeholders in the AML/CFT framework.

104. Further deficiencies with regard to the understanding of ML/TF risks are related to the assessment of ***the risks related to the abuse of legal persons***. While, unlike other chapters of the NRA 2021, the respective chapter of the report does not descriptively or numerically assess threats, vulnerabilities and risks in this area, it refers to established facts of inaccurate BO information in the BR, existence and use of shelf, shell and buffer companies, tendency of establishing Estonian private limited companies by non-resident BOs, and practice of intentional bankruptcy to avoid seizure of assets. This does not amount to a comprehensive assessment of the significance of misusing legal persons in Estonia, in terms of estimates on reliability of information in the BR, analysis on the number/ share of companies beneficially owned by foreigners/ individuals unrelated to the Estonian economy, including e-Residents, estimates on the number of companies with complex ownership structure to facilitate hiding of beneficial ownership, analysis on the involvement of CSPs in the establishment of shelf/shell/ buffer companies and their use for laundering domestic and foreign proceeds of crime.

105. Another area, where the understanding of ML/TF risks needs major improvement is the ***risks related to the e-Residency program***. Here again, the respective chapter of the NRA 2021 does not descriptively or numerically assess threats, vulnerabilities and risks associated with the program. It concludes though that e-Residency allows foreigners to use Estonia for undesirable purposes by hiding the real substance and purpose of their activities, as well as the beneficial owners of the companies established by them. This is especially problematic with regard to third countries, with which Estonia does not have cooperation relations in the field of justice, security, or law enforcement, meaning that competent authorities cannot obtain reliable information on applicants from such countries or effectively prosecute their criminal conduct. There are no estimates on and analysis of the share of e-Residents from higher risk countries, description of enhanced measures applied with regard to them, analysis of the risk exposure of Estonian financial and non-financial sectors emanating from the misuse of e-Residency program (including

through digital ID holders committing crimes or giving the ID card to another person), statistics on materialized risks due to the program (e.g. use of accounts of individuals and companies established by e-Residents for ML/TF as ascertained by STRs, EFIU analyses, investigations, prosecutions and convictions).

106. Similar deficiencies are found in the NRA 2021 analysis of the ***risks associated with activities of CSPs and VASPs***. EFIU's analyses on CSPs (2021) and VASPs (2022) go further in terms of identification and analysis of ML/TF risks emanating from these two high risk segments of the Estonian economy. The analysis on CSPs identifies the practiced activity of establishing and selling shelf/shell companies among licensed and non-licensed CSPs, low awareness in AML/CFT matters, incomplete risk management systems, insufficiently applied measures of due diligence, and poor compliance with the obligation of reporting STRs, thus making the country quite vulnerable in regard to corporate transparency and misuse of legal persons for criminal purposes. At that, the analysis regarding basic and beneficial ownership of Estonian companies cannot be considered fully reliable due to inconsistent and contradictory information (see IO.5 for further details). The analysis on VASPs identifies a lack of meaningful presence of many VASPs in Estonia, failure of the majority of market participants to implement monitoring systems and internal controls, outsourced services of client identification, practical impossibility to execute supervisory proceedings in cases where the employees of the VASP are not located in Estonia. At that, the analysis regarding the number of clients, the volume of transactions, as well as internal controls, including risk classification of customers and application of CDD measures, is based merely or predominantly on the data presented by those VASPs, which responded to the respective EFIU questionnaire, thus questioning whether the real significance of the problem has been reliably grasped.

107. Estonia's exposure to the **risk of terrorism financing** is perceived and considered primarily in the context of the risk of terrorism, which is reportedly low. The NRA 2021 analysis of the ***TF threats*** refers to one conviction achieved in 2016 regarding two individuals prosecuted for the crime of terrorism financing, along with general statements reading that *"terrorist financing is not related to predicate offences"*, *"cash flows are irrelevant in the context of terrorist financing as small amounts suffice to finance terrorism"*, and concluding that *"the national threat level in terms of terrorist financing is below average"*. The same is true with regard to analysis of ***TF vulnerabilities*** assessed average, which refers to the ISS mandate for investigating TF offences and concludes that *"the primary vulnerability is the transactions via virtual channels, as they are difficult to identify and process"*.

108. Among further efforts towards better understanding of TF risk, the authorities refer to the collection and analysis of cross-border transactional activity data through the Risk Dashboard created in 2020. The Risk Dashboard uses data from the banks' regular monthly reporting to the Bank of Estonia (BOE) on cross-border payments and to the EFSA on deposits by non-residents[111]. Monitoring is conducted against the "List of countries with higher risk of terrorism" jointly developed by the EFIU and the ISS, which partially comprises the FATF Lists of high-risk and other

[111] Aggregated data is collected on total and average incoming and outgoing cross-border transfers, cash withdrawals and card payments by country (top 10) and by bank (top 7), as well as total deposits by client residency (top 10) and by bank (top 7).

monitored jurisdictions[112]. Collected data is then compared with the imports, exports and tourism parameters to identify significant changes over time. While agreeing that this exercise could provide useful insights into cross-border flows potentially related to ML[113], the AT does not see how in practice it would facilitate, or has facilitated, identification of existing or potential risks of TF (as TF-related movements are not measured by millions or billions of EUR/ other currency). Monitoring total and average cash withdrawals and card transactions, in turn, would create value in terms of TF risk detection if supplemented by analysis of individual withdrawals or transactions based on a set of criteria/ red flags[114]. The authorities have not provided further information on, including examples of, successful use of the Risk Dashboard analytical products for identification, investigation and prosecution of terrorism or TF-related activity.

109. Overall, the understanding of TF risk is focused around the notion that activities aimed at terrorism financing are unlikely in the "raising" and "using" stages of TF. Such understanding is not supplemented by demonstrable awareness of intelligence and investigative agencies about the financial activity of individuals, groups and organisations potentially interested in infiltrating the AML/CFT system of Estonia especially in the "moving" stage of TF, as well as by the express ability to trace TF-related transfers and cash movements. Discussions on these topics during the onsite did not give a comprehensive view of the intelligence work, which has enabled conclusions of the NRA 2021 about the below average threat of TF or average vulnerability to TF, nor did they provide the vision of competent authorities regarding factual and potential risk of TF unrelated to the perception of the low risk of terrorism in the country. All of these are factors necessitating further efforts towards appropriate identification and reliable assessment of TF risks in Estonia.

110. With regard to **law enforcement efforts** towards identification and assessment of ML/TF risks, the authorities advise that while methods and tactics used by LEAs are confidential, all available information is used to compile annual situational pictures and threat or risk assessments in the field of serious hidden crime. Among them, the ISS is reported to make operational risk assessments twice a year, and a strategic analysis once per year; however, the outcomes of these assessments in the form of relevant analysis and conclusions have not been provided to the assessment team referring to confidentiality reasons (classification as state secret). A document prepared by the PBGB in December 2021 and titled *"Situational picture of money laundering crimes"* covers the period 2015-2021 and, as such, is a historical reflection on crime rates and some financial data rather than a situational picture of current ML threats or risks demonstrating competent authorities' awareness of the scope and significance of the main risk drivers and actors. While the document does not contain analysis or conclusions that might qualify as state or other secrets, it presents controversial data on the estimated domestic proceeds of crime[115], is unclear about the estimated foreign proceeds of crime passing through

[112]https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

[113] Provided that monitoring is done not only against the list of higher TF-risk countries, but for all countries/ key trade partners of Estonia.

[114] E.g. proximity to conflict zones, transactional activity indicating one-way trips or long stays in such zones, etc.

[115] For example, it concludes that the estimated volume of domestically generated money at risk of being laundered in fraud, embezzlement and drug-related crimes totals EUR 30 million per year, which in principle does not reconcile with the SRA 2021 estimate of the potential proceeds of these crimes ranging between EUR 77 to 110 million.

Estonia[116] and, overall, does not measurably contribute to better understanding of ML/TF threats emanating from domestic and foreign proceeds of crime.

111. Among the recent activities of other authorities aimed at identification of risks in the areas of interest, one should mention the ***EFSA's special project (ORTO)*** conducted in late 2018 and early 2019 inspecting all banks and branches to obtain a better overview of the measures taken by them to identify, assess and mitigate risks, as well as the functioning of control systems and the role of the management board in the AML/CFT system. The results of the inspections were summarized for each bank in meetings between their senior executives and members of the Management Board of the EFSA, and fed into their risk profiling by the EFSA. Another good example of forward-looking risk identification activity is ***EFSA's analysis of risks related to VASPs*** in the Estonian financial sector conducted in 2021. The analysis concludes that, while the risk to the Estonian banking sector in providing virtual currency services as a whole is rather low, some of the banks facilitate a very significant volume of transactions in current business relationships with VASPs (e.g. EUR 30.1 billion, including EUR 146.8 million transactions of clients with valid Estonian VASP license), whereby the banks are not always able to distinguish between everyday activities or conventional payment transactions and those related to the provision of virtual currency services.

2.2.2. National policies to address identified ML/TF risks

112. The authorities advise that the primary AML/CFT policies in the country are the action plans developed on the basis of the NRA findings. The MLTFPA mandates the AML/CFT Committee to prepare such plans of measures and activities aimed at mitigating the risks identified by the NRA, to designate the authorities that apply the risk mitigation measures and carry out relevant activities, as well as to establish time limits within which the measures must be applied, and the activities must be carried out. So far, the authorities have developed two action plans – the first based on the NRA covering the period 2011-2013, for which the plan of actions to be implemented over 2016-2017 was endorsed in March 2015, and the second based on the NRA covering the period 2017-2019, for which the plan of actions to be implemented over 2021-2024 was endorsed in July 2021. Hence, the current approach and practice of developing and endorsing action plans do not provide for uninterrupted availability of nation-wide AML/CFT policies based on timely generated and up-to-date outcomes of nation-wide risk assessments.

113. It is worth mentioning that among measures aimed at achieving 23 goals of the first Action Plan, which built on the conclusions of the NRA 2015 report, the predominant majority were awareness raising and capacity building activities targeting the competent authorities and the private sector[117]. In contrast, the second Action Plan, which builds on the conclusions of the NRA 2021 report, sets 47 goals to be achieved in relation to an identical number of issues identified by

[116] For example, it states that in all ML cases registered by the PBGB over 2015-2021, the estimated amount of assets suspected of being laundered has been EUR 1.44 billion, including EUR 1.32 billion channeled through Estonian financial institutions in cases commenced over 2017–2019 (related to Danske and other schemes) and EUR 29.6 million involved in cases commenced over 2020-2021, thus giving no idea about the current state of things as far as cross-border movements of potential proceeds of crime are concerned.

[117] Several activities of the Action Plan for 2016-2017 were related to legislative and institutional changes in the AML/CFT framework, which could not be implemented due to the lack of a relevant mechanism in the law. Accordingly, the organisational aspect of conducting NRAs and implementing their recommendations was introduced into the MLTPFA, which now establishes conducing and updating NRAs as a statutory obligation of the AML/CFT Committee.

the NRA, through activities that concern four domains (legislative, policy-making, implementation, and international cooperation)[118] and are categorized by priority (very high, high, average, and low) [119]. Implementation of the activities under the Action Plan is distributed among ministries, supervisory authorities and agencies, specifying the lead authority responsible for the activity, and the partner authorities, which share responsibility for the given activity. AML/CFT Committee oversees implementation of the Action Plan through hearings at its regular meetings.

114. With regard to the prioritisation of the activities defined by the Action Plan, it is not clear whether "priority" is construed in terms of implementation as soon as possible (since many actions categorised as low priority have the same implementation deadline with the ones categorized as very high or high priority), allocation of as much resources as possible (since there is no indication of human and other resources to be allocated for implementation of activities based on their priority), involvement of as many agencies as possible (since there is no obvious correlation between the determined level of priority and the number of partner authorities supporting the lead authority). Hence, there is a need to clearly define the notion of priority regarding activities in the Action Plan, and make relevant institutional and organisational arrangements for their priority-based implementation.

115. Looking at the composition of the activities set out in the Action Plan, it is striking that as many as 11 activities, or 23% of the total, are aimed at tackling threats and vulnerabilities related to virtual currencies and VASPs. In fact, this group of activities is the only one categorised by the AML/CFT Committee as very high priority. At that, one activity stipulating for improvement of the licensing regime of the VASPs through establishing higher barriers to market entry pertains to both legislative and policy-making domains. Then, three activities providing for introduction of additional CDD and compliance requirements for VASPs, as well as for analysis and resolution of the problem related to seizure of VA pertain to the legislative domain. Further on, six activities stipulating for analysis of low reporting performance of VASPs, ways for monitoring and identification of suspicious transactions, risks and threats related to unregulated virtual currency markets, mixing services, decentralized/ anonymous virtual assets and services left out of the scope of MLTFPA pertain to the policy-making domain. Finally, one activity providing for collection of relevant statistics and implementation of a full-scale periodic monitoring system of the customer base of VASPs pertains to the implementation domain.

116. The authorities advise that, within the group of activities categorized as very high priority, those in the legislative domain related to stricter licensing, additional CDD and compliance requirements for VASPs have already been implemented with the amendments to the MLTFPA, which have entered into force on 7 March 2022, i.e., five weeks before the onsite visit. Moreover, almost all activities in this group pertain to the policy-making domain with implementation deadline of 2022-2023 and are in essence a learning exercise aimed at further exploration of the issues identified by the NRA 2021 in order to understand their scope and significance, so as to inform future decisions on the possible ways for dealing with them. This, on one hand, confirms

[118] Among activities defined by the Action Plan, 10 pertain to the legislative domain, 17 – to the policy-making domain, 20 – to the implementation domain, and 1 – to the international cooperation domain (the sum total is more than 47 as some activities pertain to more than one domain).
[119] Among activities established by the Action Plan, 11 are considered very high priority, 7 – high priority, 3 – average priority, and 26 – low priority.

the assessment team's conclusion about the limited ML/TF risk understanding of the authorities and, on the other hand, indicates the need for accelerating conduction of the learning exercise in order to update the national AML/CFT policy with specific and focused activities in the implementation domain addressing identified ML/TF risks. Overall, it is hard to make judgments about the factual extent of implementation of activities defined by the Action Plan, since besides the above-mentioned amendments to the MLTFPA, most activities are marked as "in progress" with implementation deadlines over the next two-three years, or there is no indication of the advancement stage in terms of factual implementation.

117. The assessment team considers that, in relation to a number of issues identified both by the NRA or other strategic analysis products and by the assessment team as creating high exposure to ML/TF risks, certain areas have not received proper attention in the Action Plan – in terms of either due priority or commensurate action – in a way to comprehensively address these issues in the foreseeable future. This concerns, *inter alia*, proper estimation of criminal proceeds, existence of Supreme Court rulings suggesting a narrow interpretation of the ML offence, insufficient capacity of competent authorities to address e-Residency risks, incomplete overview of the state in a number of sectors, and lack of the EFIU resources vis-à-vis its tasks.

118. The Action Plan defines the high priority issue related to ***proper estimation of criminal proceeds*** as *"the state has an incomplete overview of the estimated extent of criminal proceeds"* with implementation deadline of 2021-2022. The authorities advise that this issue relates to the ARO in the PBGB, particularly to its capacities and processes in criminal investigations (although this does not derive from specific analysis and conclusions in the NRA 2021). To deal with this issue, it establishes to carry out analysis for determining the estimated level of criminal proceeds and deciding on the allocation of additional resources, so that a sufficient number of officials are in charge of combatting crimes. While the assessment team confirms the lack of comprehensive analysis on domestic and foreign proceeds-generating crimes, as of the time of the onsite visit the authorities did not report measurable progress or interim outcomes of the relevant analysis, nor advised on preliminary decisions on resource (re)allocation initiatives towards addressing this issue with a key role in the overall AML/CFT framework.

119. The high priority issue related to the ***existence of Supreme Court rulings suggesting a narrow interpretation of the ML offence*** is defined as "*[…] interpreting the composition of the money laundering offense is not in accordance with international standards and unreasonably narrows the definition of ML, imposed penalties are not sufficient, intentional non-application of due diligence measures facilitates ML and TF"* with implementation deadline of 2022-2023. The respective activity for dealing with this issue stipulates: 1) to analyse the need for specifying the necessary elements of the ML criminal offense, and for criminalizing the so-called institutional ML, also known as intentional non-application of due diligence measures; and 2) to establish and align administrative fine rates and their processing with the EU AML Directive. As described in the analysis for Core Issue 1.1, the vulnerability due to restrictive interpretation of ML offence by the Supreme Court rulings has very significant effectiveness implications (see the analysis under IO.7 for further details), and the action to analyse the need of remedying that vulnerability is not a commensurate response to this vulnerability. Moreover, the effect of complexities in addressing infringements of AML/CFT obligations through misdemeanour proceedings is an issue identified since the first Action Plan endorsed in 2015, again with significant effectiveness implications deserving more specific and urgent action.

120. With regard to the low priority issue related to ***insufficient capacity of competent authorities to address e-Residency risks*** defined as *"supervisory authorities and law enforcement agencies do not have sufficient resources to address e-residency risks, related risk mitigation is difficult"* with implementation deadline of 2021-2024, the Action Plan provides as many as seven activities, including creation of additional positions within the EFIU and the ISS, obliging service providers to monitor use of digital IDs, and establishing the right of the state to revoke digital IDs if misused, thus confirming the conclusions of the assessment team about the gaps and related risks of the e-Residence program. Nonetheless, the low priority of this issue, also reflected in the long implementation period does not demonstrate that the state acknowledges – and is willing to tackle as soon as possible – the significant risks associated with the e-Residency program.

121. Another low priority issue identified in the Action plan concerns ***incomplete overview of the state in a number of sectors***, defined as *"the state has an incomplete overview of what is happening in many sectors"* with implementation deadline of 2024. To deal with this issue, the Action Plan stipulates to establish an obligation for designated professionals, NPOs, CSPs, crowdfunding service providers and VASPs to submit reports to the supervisory authority. The assessment team considers that the low priority and distant deadline of implementation of this activity fail to appreciate major threats and subsequent risks related to the CSP sector in general, do not reconcile with another activity classified as very high priority and stipulating to establish a "full-scale monitoring system" of VASPs and, as such, do not constitute proper response to the risks identified through the NRA and other strategic analyses in these sectors.

122. Regarding the low priority issue with ***the lack of the EFIU resources vis-à-vis its tasks*** defined as *"the EFIU does not have enough resources to cover all the necessary activities"* with implementation deadline of 2022, the Action Plans prescribes that the EFIU should analyse the priority of its activities, review its resources and request additional resources as needed for supervision, preparation of guidance materials, training and creating more effective partnership with market participants. While classifying this activity low priority seems to undermine the importance of supervisory function of the EFIU over the highest risk sectors of VASPs and CSPs (in addition to numerous other sectors supervised by the EFIU), as of the time of the onsite visit the authorities did not report measureable progress or interim outcomes of the relevant analysis, nor advised on preliminary decisions on additional resource allocations towards addressing this important issue[120].

123. Among national strategies and policies relevant for combating ML/TF, the authorities refer to the Strategy "Estonia 2035", the Fundamentals of Criminal Policy 2030, the Internal Security Strategy 2020-2030, the Foundations of Security Policy of Estonia, the Anti-Corruption Strategy 2025, the Priorities in the Fight Against Crime (from 2022), the Strategy of the PBGB until 2030, the Strategy of the EFIU for 2022–2026, and the EFSA Operating Strategy for 2019-2021, which, to a varying level of focus and detail, define strategic goals, such as improving competence to fight serious covert crimes, preventing corruption and economic (including ML) crime, enhancing identification and confiscation of criminal proceeds, strengthening capacity to identify terrorist risks, raising awareness of ML/TF risks, and implementing risk-based supervision towards further improvement of the AML/CFT system in the country. Some of these policies and strategies

[120] The authorities advice that on 1 June 2022 the EFIU requested for additional funding from the state budget

have had relevant predecessors for earlier periods, as well. While admitting that implementation of these high-level strategic documents would overall contribute to enhanced effectiveness of the national AML/CFT system, the assessment team considers that these documents do not qualify as national AML/CFT policies insofar as they do not provide focused and targeted actions towards mitigation of ML/TF risks identified by the NRA or other strategic analysis products. Based on the facts and circumstances analysed above, the assessment team is not in a position to conclude that identified ML/TF risks are effectively addressed by national AML/CFT policies.

2.2.3. Exemptions, enhanced and simplified measures

124. The current legislation provides for some exemptions from FATF Recommendations requiring DNFBPs to take certain actions. In particular, according to MLTFPA, competent supervisory authorities may, at the request of the obliged entity, except for those supervised by the EFSA, i.e. credit and financial institutions, decide that the preparation of a documented risk assessment[121] is not mandatory having regard to the NRA and where specific risks of the respective sector are clear and understandable, or where the risk assessment prepared by the supervisory authority or the NRA has established risks, risk appetite and risk management model of the respective sector, and the obliged entity implements these. The authorities advise that such exemption has been requested only once by auditors and declined by the EFIU.

125. According to MLTFPA, the obliged entities should establish rules of procedure that allow for effective mitigation and management of ML/TF risks as identified in their documented risk assessments. Such rules of procedure should set out the measures applied within SDD and EDD. MLTFPA sets out that the obliged entity, except for a credit institution or financial institution, may apply to the competent supervisory authority for partial or full release from the obligation to prepare documented rules of procedure and internal control rules having regard to the NRA, the nature, scope and level of complexity of the obliged entity, and whether specific risks related to the obliged entity are small or effectively managed. The authorities advise that such exemption has never been requested and granted.

126. In addition, according to MLTFPA the following categories of entities are exempted from the AML/CFT framework. Those are: (i) the persons engaged in buying-in or wholesale of precious metals and precious metal articles used for production, scientific or medical purposes; (ii) an insurance undertaking providing services related to mandatory funded pension insurance contracts within the meaning of the Funded Pensions Act; and (iii) a management company upon managing a mandatory pension fund within the meaning of the Funded Pensions Act, and an investment fund founded as a public limited company within the meaning of the Investment Funds Act. Those exceptions are not supported by substantive assessment of ML/TF risks concluding that there is a proven low risk in those sectors or activities, and that those exceptions occur in strictly limited and justified circumstances.

127. Obliged entities are allowed to apply SDD and required to apply EDD measures in situations where, based on the risk assessments mentioned above (which, in turn, should consider the NRA) they establish, respectively, a lower or higher risk of ML/TF. Factors of lower and higher risk set out in MLTFPA in essence replicate the non-exhaustive lists of factors and types of evidence of

[121] As required under FATF R.1, criterion 1.10 and MLTFPA Section 13(1).

potentially lower or higher risk set out in the FATF INR 10, as well as Annexes II and III of the EU AML Directive. The authorities advise that, upon endorsement and publication of the NRA 2021, series of meetings and other communication have been organized with the private sector to introduce the outcomes of the NRA, as well as other risk assessments and strategic analyses (such as the SRA conducted by the EFSA (2021), analyses conducted by the EFIU on CSPs (2021) and VASPs (2020 and 2022)), presenting their findings on higher risk sectors, activities and actors in Estonia to be subjected to EDD measures.

2.2.4. Objectives and activities of competent authorities

128. As described in the analysis for Core Issue 1.2, the primary AML/CFT policies in the country are the action plans developed on the basis of the NRA findings. All competent authorities have a role – either as a lead or a partner authority – in the implementation of the activities established under the most recent Action Plan endorsed by the AML/CFT Committee in July 2021, which builds on the conclusions of the NRA 2021 report and sets the goals to be achieved in relation to the issues identified by the NRA. The authorities advise that, since the AML/CFT Committee is responsible for overseeing implementation of the Action Plan (through semi-annual monitoring), from organisational point of view they have seen no need to incorporate the objectives and tasks of the Action Plan into the strategies and work-plans of individual agencies, unless this is considered appropriate for internal purposes.

129. Accordingly, strategies and work-plans of the competent authorities (as much as provided to the assessment team), with some reservation for the 2022 work-plan of the EFIU, do not provide for specific tasks and relevant resources to be channelled to the implementation of the activities defined by the Action Plan. This means that, at least for some of the competent authorities, these activities would remain a "facultative" work to be carried out as much as circumstances allow that – a situation that the authorities faced in the course of conducting the NRA, where members of the project performed their tasks significantly increasing workload as a side-work to their main job, and not everyone had the time or willingness to sufficiently contribute to the project. In that regard, it is an important gap that outcomes of nation-wide risk assessment exercises are not integrated into the objectives and activities of individual authorities, by adjusting agency-level policies and driving institutional or operational changes focused on identified or emerging ML/TF risks.

130. All authorities confirm to have acted on a risk-sensitive basis throughout years. To exemplify this, references are made to the cases of four credit institutions and one PSP, with regard to which: 1) the EFSA has since 2015-2016 enforced exit from certain products and customer categories, revoked (or initiated revocation of) activity licenses, issued precepts, achieved change of business model and management, and made criminal reports to the LEAs; 2) the EFIU has since 2017-2018 received (or enforced filing of) thousands of STRs, made and responded to numerous requests to/ from foreign counterparts, made disseminations to domestic LEAs to support criminal investigations; 3) the LEAs have initiated since 2017-2018 some criminal (pre-)investigations based on crime reports from the EFSA, and made and responded to numerous EIOs and MLAs to/from foreign jurisdictions, brought charges against tens of individuals accused for facilitating movement of several billions of suspicious funds through the Estonian financial system, identified and secured for confiscation of several millions

of funds in Estonia and abroad. As of the time of the onsite visit, no convictions were achieved further to the mentioned investigations and indictments.

131. Without diminishing the scale and significance of the measures taken by the authorities over the last 6-7 years towards changing the "rules of the game" and enforcing a more transparent system with a higher level of integrity, the steps described in the above paragraph hardly amount to *"activities of the competent authorities …consistent with the evolving national AML/CFT policies and with the ML/TF risks identified",* for two reasons. First, the NRA covering the period 2011-2013 and endorsed in January 2015 as the outcome of the nation-side ML/TF risk assessment, whilst describing in general terms non-resident business in individual banks as one of the highest risks, did not reflect even a fraction of the factual ML/TF risks materialised in the financial sector immediately before and during the time of conducting the NRA. Also, the Action Plan endorsed in March 2015 as the national AML/CFT policy was by far inappropriate to address the mentioned risks. Second, activities of the competent authorities, with some reservation for the ones initiated by the EFSA[122], have not proven to be a proactive response aimed at addressing timely and properly identified ML/TF risks. Considering the long period of time, in which extremely significant ML/TF risks existed and materialised in the country (since 2006-2007 or earlier until at least 2016-2017), the part of the authorities' activities related to dealing with the multinational "laundromats" in the recent past, be it in intelligence, supervision or law enforcement domains, has not had the required impact in due time and does not count into the effective implementation of the FATF Standard as far as Core Issue 1.4 is concerned.

132. Regarding the time period since 2016-2017 up until now, the assessment team considers that identification of ML/TF risks and development of national AML/CFT policies need major improvements, due to the reasons articulated in the analysis for Core Issues 1.1 and 1.2 above. Particularly, the missing elements in the present understanding of the ML/TF risks coupled with the issues not appropriately dealt with in the current national AML/CFT policy allow generation of new risks, or do not provide for mitigation of the existing ones, insofar as the activities of the authorities are not proactive, timely and decisive enough to preclude another cycle of reactive responses to already materialised risks within the next years. This concerns, first of all, the e-Residency program, activities of CSPs and VASPs, as well as the risks related to a special cluster of customers (VASPs, PSPs and EMIs).

133. With regard to the ***e-Residency program***, as one of the first countries to have introduced such a program Estonia has not implemented measures to ensure that it knows, to a sufficient extent of confidence, who the Estonian e-Residents are and to whom it has issued the Estonian digital identity, what kind of ML/TF and other threats emanate from the holders of such identity. This and other gaps identified since the audit conducted by the Parliament's National Audit Office in 2020 indicate that the program makes Estonia vulnerable to perpetrators from foreign jurisdictions, who might use their Estonian digital identity for illegitimate purposes both in the country and abroad. As described in Chapter 1 of this report, the problem concerns e-Residents from both EU countries (see the example regarding Finnish nationals) and those from third

[122] In particular, activities of the EFSA through (i) inspections in a credit institution in 2014-2015 and the subsequent enforcement actions to discontinue non-resident business, (ii) inspections in another credit institution in 2015-2017 and subsequent withdrawal of license by the ECB for AML/CFT failures, as well as (iii) closure of another non-resident business in 2017 in a bank whose activities were uncovered by leaks in 2019.

countries, with which Estonia does not have cooperation relations in the field of justice, security, or law enforcement. Nevertheless, the authorities have not demonstrated targeted actions taken since then to remedy the gaps of the program, and the deficiencies identified by the assessment team further prove materiality of these gaps in terms of, *inter alia*, materialising risks with the misuse of the companies established or controlled by e-Residents.

134. Regarding ***activities of CSPs***, facts about licensed and non-licensed Estonian CSPs extensively involved in establishing and selling shelf/ shell companies were widely known even before the EFIU's analysis of CSPs published in 2021, which confirms that Estonia as a jurisdiction is quite vulnerable in regard to corporate transparency and misuse of legal persons for criminal purposes. As also referenced in Chapter 1 of this report, the so-called multi-service providers offer the whole range of services aimed at concealing beneficial ownership, including appointment of nominal directors and shareholders. The amendment to the Commercial Code effective from January 2019 removing the requirement for private limited companies to use an Estonian bank account when registering share capital extends the geography of the problem[123]. In this regard, measures taken by the authorities towards mitigation of the risks emanating from CSP activities have been by far insufficient. For example, whenever the PBGB identifies a non-licenced CSP facilitating the application for e-Residency, it sends a notification reminding the CSP that the activity is subject to authorization by the EFIU, without sharing that notification with the EFIU for follow-up action. The measures implemented through March 2022 amendments to the MLTFPA abolishing the exemption for CSPs from applying due diligence measures upon making or mediating occasional transactions outside a business relationship, including in the occasional sale of a ready-made company, still have to prove being effective.

135. As regards the ***activities of VASPs***, as one of the first countries to issue licences for VASP activity since the end of 2017, Estonia at least until very recently has not taken adequate measures to ensure proper regulation and supervision of the VASPs holding Estonian licences. In essence, for a long period of time and until very recently (mid-2021) issuance of a VASP license has been a rather technical process almost always facilitated by CSPs and amounting to an act of recognition/ registration of existence rather than a procedure implementing substantial market entry rules and control practices. In this regard, the authorities response, after the FATF updated its assessment Methodology on VASPs in October 2019, to materialised risks through March 2020 amendments to the MLTFPA introducing a requirement for VASPs to have a management body and place of business in Estonia proved inefficient, as the market participants quickly found a way to circumvent this requirement by appointing nominal management and obtaining a formal address in the country. The next action in response to evolving risks related to VASPs came two years later, through March 2022 amendments to the MLTFPA introducing stricter licensing, additional CDD and compliance requirements for VASPs, which still have to prove being effective.

136. With regard to the ***risks related to a special cluster of customers***, a new trend over the last years is the provision of payment services in the context of correspondent relationships to clients, which are FIs and VASPs using current accounts or fund products to service their own customers. In order words, these are services where the accounts with a credit institution are not used directly by the customer who has a business relationship with the credit institution, but by

[123] This change means that all private limited companies incorporated in Estonian may conduct their business activity using any business account opened with a credit or payment institution from across the Europe Economic Area.

the customers of that customer. It appears that, compared to the period before 2015-2016 when information surfaced on major involvement of some Estonian banks in multinational "laundromats", the risk of ML related to the non-resident business mainly involving cross-border transfers through the Estonian financial system has observably "relocated" from most of the banking sector to those of VASPs, PSPs and EMIs along with certain "conversion" back to the former through services provided to them (e.g. EUR 30.1 billion in current business relationships with VASPs in 2021). These include nested and payable-through accounts of VASPs, PSPs and EMIs (including through VIBAN services provided by Estonian banks) that might be serving tens or hundreds of thousands of own customers, whose identification and transaction monitoring are not in the capacity of the provider of correspondent service.

137. To summarise the analysis of the extent to which objectives and activities of the competent authorities are consistent with the evolving national AML/CFT policies and ML/TF risks identified, the assessment team considers that in some cases, such as the e-Residency program or the VASP licensing, the authorities have not implemented sufficient measures to identify potential ML/TF risks before the launch of the respective initiatives and to take timely actions towards mitigation of the risks that have surfaced – and will inevitably evolve – in the course of realising these initiatives. In other cases, such as the CSPs, the authorities have failed to take decisive and timely action regarding major and continuing ML/TF risks materialising in different environments and circumstances. These deficiencies are amplified by the lack of systemic approach and consistent action in Estonia for the alignment of objectives and activities of competent authorities with national ML/TF policies, as described in the beginning of the analysis for this Core Issue.

138. Given the limited information available on the advancement stage in terms of implementing the Action Plan, the assessment team cannot make informed conclusions as to whether its implementation would result in focused action of the competent authorities consistent with identified ML/TF risks towards, *inter alia*, better intelligence output and guidance by the EFIU, more effective oversight of obliged entities for compliance with the AML/CFT requirements by the supervisors, and improved practices of combating major domestic and foreign ML/TF threats by the LEAs.

2.2.5. National coordination and cooperation

139. The AML/CFT Committee[124] chaired by the Minister of Finance and comprised[125] of the high-level representatives of ministries, law enforcement agencies, the Prosecutor's Office supervisory authorities and the EFIU is the primary mechanism for AML/CFT cooperation and coordination at the national level. Competences of the committee include coordinating preparation and updates of the NRA, preparing relevant action plans with established deadlines for implementation, organising and overseeing their implementation, making proposals for

[124] The committee was established on 19 April 2018 by Regulation No. 34 of the Government of Estonia.

[125] The members of the committee are the Secretary General of the MoJ, the Secretary General of the Ministry of Interior, the Undersecretary for Financial Policy and Foreign Relations of the Ministry of Finance, the Undersecretary for Political Affairs of the Ministry of Foreign Affairs, the Head of the FIU, the member of the Management Board of the Financial Supervision Authority, the Undersecretary of Communications and State Information Systems of the MEAC, the Director General of the Police and Border Guard Board, the Prosecutor General, the Director General of the Tax and Customs Board, the Director General of the Internal Security Service, and the Deputy Governor of Eesti Pank.

legislative amendments, and pursuing national cooperation in AML/CFT and in countering proliferation. The committee holds regular meetings, adopts decisions through resolutions by majority voting, and produces minutes of meetings that are endorsed by the members. Based on the contents of the minutes of meetings, as well as the discussions with the AML/CFT Committee members the assessment team is in a position to conclude that all significant matters related to the AML/CFT framework in the country are brought before the committee for substantial discussion, and important decisions are made on the way forward.

140. The AML/CFT Committee is entitled to create ad hoc working groups for specific tasks. This was done in November 2018, by creation of two ad-hoc working groups to examine institutional and procedural aspects of the AML/CFT framework in the country. After seven months of work, the working groups made proposals to the AML/CFT Committee, particularly: 1) regarding the institutional framework – on developing the function of the Strategic Analysis Center led by the EFIU; creating a legal basis for sharing the data of Eesti Pank with the competent authorities; introducing into the MLTFPA additional due diligence requirements for CSPs; and allocating additional resources to the EFIU, the PBGB (Economic Crime Unit), the Prosecutor's Office, the MoF and the MoJ; and 2) regarding the procedural framework – on regulating whistle-blower protection more uniformly and horizontally; considering obstruction of supervisory activities as a criminal offense (vs. misdemeanour); tackling the risk of the misuse of companies; introducing the institute of administrative fines (vs. the institute of misdemeanour proceedings); and ratifying the Warsaw Convention.

141. In June 2019, the AML/CFT Committee considered and endorsed the proposals made by the working groups, after which they ceased to exist. The authorities advise that most of the proposals were implemented by making relevant amendments to the MLTFPA in 2020 and 2021, or initiating changes in the structure of relevant agencies. At that, some of the proposals, such as the one on introducing the institute of administrative fines (vs. the institute of misdemeanour proceedings), which are also defined as activities under the Action Plan endorsed by the AML/CFT Committee in July 2021, are still very relevant in terms of enhancing effectiveness of sanctioning measures for non-compliance of obliged entities with requirements on preventative obligations set out in the MLTFPA and other enforceable means.

142. The Operational Working Group established under the AML/CFT Committee in January 2022 would mainly focus on cooperation between the EFIU, the LEAs and the EFSA to work out operational matters relevant for AML/CFT. The Operational Working Group is led by the EFIU and has representatives from the ETCB, the PO, the ISS, the PBGB (Central Criminal Police) and the EFSA. Where necessary, the EFIU may change the composition of the working group to engage with a specific matter. The assessment team is not in a position to make conclusions on the role and contribution of the Operational Working Group to the enhancement of effectiveness of coordination and cooperation at national level, due to its very recent establishment.

143. Another structure aimed at ensuring national coordination and cooperation is the Market Participants Advisory Committee[126]. As a sub-committee of the AML/CFT Committee, the MPAC

[126] Membership of the MPAC comprises representatives of: the Banking Association (chairing authority), the Network of Non-Profit Organizations, the Chamber of Bailiffs and Trustees in Bankruptcy, the BA, the Association of Accountants, the Association of Real Estate Firms; the Gaming Operator Association, the Auditors Association, the CN, the

comprises also representatives of the SRBs, i.e., the CN and the BA. The MPAC meetings are organised in connection (shortly before or after) the meetings of the AML/CFT Committee, while the chair of the MPAC attends the meetings of the AML/CFT Committee, except for confidential agenda items. This enables that information from the AML/CFT Committee, including on the implementation of the Action Plan as the national AML/CFT policy, is made available to the members of the MPAC, including the SRBs.

144. The authorities advise that there are two more structures – the Security Committee of Estonia and its subdivision, the Counter Terrorism Council – with a mandate in matters related to combating terrorism. It is not clear, though, whether these structures have a specific role or tasks related to combating TF.

145. According to the MLTFPA, competences of the AML/CFT Committee include "countering proliferation", but not the financing of proliferation, and it is not clear what specific tasks are performed by the committee towards realisation of this mandate. The authorities advise that representatives of the MFA, which leads the Strategic Goods Commission (SGC), occasionally update the AML/CFT Committee on matters related to implementation of, *inter alia*, the UNSCR 1540 on the prohibition of weapons of mass destruction, as well as on measures to control export of dual-use and military goods. The SGC is comprised of the representatives of the MFA, MOD, the Ministry of Economic Affairs and Communications (MEAC), the ISS, the PBGB and the ETCB. It appears that, upon its move out of the PBGB into the MOF, the EFIU has no more direct involvement in CPF matters considered by the SGC. The authorities also inform that there is another platform, the Steering Committee for Implementation of International Sanctions established on 27 January 2022, with a mandate to combat proliferation financing, although it is not clear how it interacts with the SGC or the AML/CFT Committee in terms of national coordination and cooperation specifically in CPF matters. The EFIU advises of having exchanged information with the SCG regarding expert advice on specific goods (in 5 occasions) and with the ISS regarding suspicions of mediation in unauthorised export of military goods (on 9 cases) over the last five years.

146. Horizontal exchanges of information on risks/trends and specific cases (other than within the framework of the AML/CFT Committee) appear to be a regular practice pursuant to the MoUs between the EFIU, the EFSA and the LEAs, supplemented by bilateral or multilateral meetings between the EFIU and the LEAs (e.g., with regional police prefectures and prosecutor offices regarding on-going investigations), and consultations in the course of conducting strategic and tactical analyses.

2.2.6. Private sector's awareness of risks

147. Financial institutions and DNFBPs affected by the application of the AML/CFT requirements were involved in the NRA process through the participation of 12 umbrella organisations and professional associations, as well as 15 market participants from the private sector in 10 working groups in charge of analysing threats and vulnerabilities in the respective sectors. Shortly after endorsement of the NRA 2021 report by the AML/CFT Committee in April

Cryptocurrency Association, the Leasing Association, Finance Estonia, the Insurance Association, the Chamber of Commerce and Industry, the Vehicle Dealers and Services Association, and the Travel and Tourism Association.

2021, it was published on the MOF website in May 2021. Thereafter, the authorities organised series of awareness-raising events for the representatives of financial and non-financial sectors to present the outcomes of the NRA 2021 through physical meetings (seminars) and via online meetings with the MPAC and the AML Committee of the Banking Association. The results on specific sectors were also circulated to the OEs through their umbrella organisations and professional associations.

148. There is no information about whether the private sector was anyhow involved in the conduction of other strategic analyses, such as the EFSA's sectorial risk assessment (2021) or EFIU's analyses on CSPs (2021). With regard to the requirement for obliged entities to integrate the outcomes of the NRA in their enterprise-wide risk assessments, the EFSA advises that a relevant question has been included in the annual off-site supervision questionnaire. While the assessment team has not been provided information on the outcomes of the analysis of responses to the mentioned question or, in a wider context, factually ascertained compliance of OEs with the MLTFPA provisions requiring to consider the outcomes of the NRA whenever they establish a lower or higher risk of ML/TF for the application of, respectively, SDD or EDD measures, other supervisors do not advise of having taken similar measures in this regard. With regard to the provision of guidance on risks identified by the NRA and other strategic analyses, the assessment team has not been provided information on specific guidance in the form of STR indicators, red flags, ML/TF typologies and trends particularly developed on the basis of the findings of the NRA and communicated to the OEs for improving awareness of the NRA outcomes.

149. Banks met onsite were well aware of the process and outcomes of the NRA (some of them had participated in it individually or through the umbrella organisation). They concurred with the key findings of the NRA, particularly about high risks associated with VASPs, CSPs and NPOs, the misuse of companies and cross-border flows of funds to/from higher risk jurisdictions. Some of them disagreed with the conclusion of the NRA about the medium high risks associated with estate brokers, considering that their activities did not amount to that of real gatekeepers, but was limited to intermediation bringing together buyers and sellers without any (fiduciary) role in facilitating relevant payments. Banks confirmed integration of the NRA findings into their own risk management/mitigation policies and procedures. DNFBPs were generally aware of the existence of the NRA, some of them through notifications by the umbrella organizations, without providing much detail on how exactly the recommendations of the NRA were implemented, or what were the specific considerations and amendments introduced into their internal regulations after the publication of the NRA. The same cannot be said about VASPs.

Overall conclusions on IO.1

150. Estonia has an appropriate mechanism for identification, assessment and, subsequently, understanding of ML/TF risks through national risk assessments, which should be significantly improved to provide for uninterrupted coverage of considered periods, as well as timely endorsement and dissemination of the assessment outcomes. The same is true for the action plans produced on the basis of NRA findings. While the NRA 2021 report and other strategic analyses provide useful hints on sectors with higher risk exposure, they do not give a comprehensive view of the (residual) risks of ML and TF in the country. Estonia's exposure to the risk of TF is perceived and considered primarily in the context of the risk of terrorism, which is reportedly low.

151. All competent authorities have a role in the implementation of the activities established under the national AML/CFT policy, i.e., most recent Action Plan. Nonetheless, outcomes of nation-wide risk assessment exercises are not integrated into the objectives and activities of individual authorities. The part of the authorities' activities related to dealing with the multinational "laundromats" in the recent past has not had the required impact in due time and does not amount to effective and timely response to existing and potential ML/TF risks. Proactive, timely and decisive actions should be taken to mitigate existing risks, especially those related to the e-Residency program, activities of CSPs and VASPs, and a special cluster of customers (VASPs, PSPs and EMIs), as well as to prevent generation of new ones, so as to preclude another cycle of reactive responses to already materialised risks within the next years.

152. National cooperation and coordination is a strong feature of the AML/CFT system in Estonia, supported by regular work of the high-level AML/CFT Committee, operational-level working groups/ platforms, as well as adequate bilateral cooperation mechanisms and practices. The framework for cooperation and coordination in the area of combating PF does not appear to be clearly defined and consistently implemented. Unlike VASPs and most of the representatives of the DNFBPs, major players in the financial sector confirm participation in the most recent nation-wide risk assessment, demonstrate awareness of its outcomes and elaborate on their integration into own enterprise-wide risk assessments.

153. **Estonia is rated as having a Moderate level of effectiveness for IO.1.**

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

a) Financial intelligence along with other relevant information is gathered and used by the competent authorities to initiate and support ongoing investigations, to develop evidence and to trace criminal proceeds. This is done to a major extent in relation to proceeds-generating predicate offences. It did appear to play an important role in counter-TF activities, when pursued.

b) The competent authorities receive reports that contain relevant and accurate information that assists them to perform their duties to a moderate extent. The reports received do not adequately reflect on the most prevalent predicate offences. In addition, high-risk sectors such as VASPs, CSPs and investment firms have consistently submitted a low share of reports throughout the period, notwithstanding their elevated risks. Retroactive reporting and a low quality of reporting has been observed. While the EFIU had recognised the issue of low-quality reporting in 2016, the feedback and guidance provided has not yet yielded appreciable results.

c) Estonia should be commended for the demonstrated practice of co-ordination and co-operation between the EFIU and LEAs, and the EFIU's efforts to meet the operational needs of the LEAs. On the other hand, a moderate improvement is required in the EFIU's capacities and working practices for reinforcing its proactive approach in the detection of targets versus its current heavy reliance on the LEA's lead. This is a priority matter in the context of Estonia, as the EFIU is in the best position to observe and detect the movement of illicit flows.

d) Sufficient formal regular feedback is not provided by the LEAs to enable the EFIU to have accurate knowledge about the outcomes of its disseminations and understanding about the relevance and utility of its work. Comprehensive statistics on the use of EFIU disseminations have not been maintained.

e) When the EFIU suspends funds, it informs the interested party of the suspension order and it practices in-person meetings with such parties in order to ascertain the origin of the funds (the latter having been addressed also in the 4th round of ME). There are some concerns in terms of revealing the operational work done by the EFIU and jeopardizing the detection of crime and the tracing of assets.

f) In recent years, important steps were taken aimed at strengthening the EFIU's capacities and its performance. The EFIU has increased its budget, human and IT resources which is commendable, but further enhancement of resources is still required. Some of the effects of the EFIU's understaffing can be seen in its written procedures for operational analysis, which take the workload of the analysts into consideration when deciding whether to analyse a report in depth.

Immediate Outcome 7

a) In Estonia, different sources of information are used to trigger ML identification and investigation. Overall, the number of identified and investigated ML cases is relatively low. ML investigations are mainly triggered by police reports and by EFIU disseminations. Even though authorities conduct parallel financial investigations and some triggered ML investigations, the proportion of those remains unclear. Whilst foreign predicate offences pose the highest threat in Estonia, MLA requests trigger domestic ML investigations only in sporadic cases. At the same time, the authorities have established practice to work through previously received MLA requests in order to identify predicate offences which led to some complex ML investigations. The agencies and specialist units appear to be reasonably well resourced, albeit there are some under staffing issues, in particular in the PO. The authorities are provided with regular training, including the judiciary and prosecutors undertake ML–related training. Co-operation between the authorities is strong.

b) In Estonia, areas identified as posing the highest threats are criminal offences committed abroad. Most of ML investigations and prosecutions relate to foreign predicate offences (with circa 70% of convictions relating to the same), with computer and internet-based fraud being the prevalent offence. Some significant cases involving banks are currently ongoing. However, concerns remain regarding whether the risks relating to domestic high-proceeds-generating offences, such as drug trafficking and organised crime, are being sufficiently considered to investigate potential ML.

c) The interpretation of the ML offence in some cases by the Supreme Court has been narrower than the legislative threshold, thus hindering further investigations and prosecutions particularly for self-laundering cases. There has, however, been mitigation of such issues and the jurisdiction does not have a binding system of judicial precedent, with separate examples given of cases which depart from these principles.

d) The majority of ML convictions are for third-party ML, mostly in relation to foreign predicate offenses (circa 70%). Several ML convictions are achieved for autonomous ML. Legal persons are rarely prosecuted and convicted in Estonia. Delays in court proceedings have occurred albeit it is not a systemic issue.

e) The criminal sanctions applied for the ML offence (both as imposed by the court after trial and as agreed in a settlement agreement) call into question their dissuasiveness and effectiveness given the gravity and associated risk. Imprisonment sentences for natural persons are low and are usually "conditional". The sanctions imposed on legal persons have been very low.

f) Estonia can apply some measures, such as extended confiscation. Nevertheless, this measure cannot be given weight as an as alternative for not achieving ML conviction since in those cases ML was not pursued at all due to the lenient sentencing practice and limitations imposed by jurisprudence.

Immediate Outcome 8

a) In Estonia confiscation is recognised as a policy objective by several high-level governmental documents, as well as by legislative and institutional framework for seizure and confiscation of instrumentalities, proceeds, property of equivalent value, and extended confiscation. The achieved results to some extent follow the set objectives.

b) Overall, authorities demonstrated making practicable steps to secure confiscation of proceeds of crime and they have achieved some reasonable results. There is discrepancy between seized and confiscated property caused by several reasons. It appears that financial investigations are regularly launched in order to trace and secure assets subject to confiscation (including extended), even though the exact number remains unclear. Laundered proceeds in specific cases were appreciably much higher than the amounts subject to confiscation. Whilst not all the funds remained in Estonia, it is not evident that Estonia has always been proactive in pursuing the remaining funds abroad. Some examples were provided of assets being shared with Estonia or repatriated but Estonia did not share any assets with foreign jurisdictions. Instrumentalities are not routinely confiscated.

c) The authorities appear to manage different types of seized assets. Nevertheless, some concerns remain about adequate capacities and measures in place for management of more complex assets such as legal persons and VAs.

d) Estonia operates a declaration system for cash above EUR 10 000 for those entering or leaving the EU. There is no such system for intra-EU transfers, nor does the declaration system extend to mail and cargo although the authorities do carry out searches generally. Sanctions applied for undeclared cash are minor and applied in the misdemeanour procedure unless the undeclared amount exceeds EUR 40 000 when criminal proceeding is initiated.

e) The Estonian authorities confiscate property, mainly through extended confiscation. However, the overall achieved results are in line to some extent with the predicate offences posing a higher ML risk according to the NRA.

Recommended Actions

Immediate Outcome 6

a) The EFIU should revise its capacities and working practices and reinforce a proactive approach in the detection of ML/TF targets on its own motion including in high-risk areas. The EFIU should, in parallel, continue providing support to LEAs within their ongoing proceedings.

b) The EFIU should revise their reporting guidelines for OEs with a view towards ensuring a more analytical and critical approach to reporting and a heightened capability of stemming the outflow of illicit funds from the jurisdiction. The EFIU should enhance feedback and trainings to OEs with a focus on higher-risk sectors to ensure the improvement of reporting practices and quality.

c) Estonia should ensure that: (a) the EFIU refrains from in-person meetings with a party whose assets have been suspended for obtaining additional clarifications; and (b) the length of the EFIU suspension orders be adjusted so as to avoid raising the need to inform the customer about the application of this measure, with a view towards ensuring that the detection of crime and the tracing of assets is not jeopardised.

d) The EFIU should improve its practices in dealing with TF-related reports and in conducting in-depth analysis of the same. It should better integrate and exploit all the different types of reports it receives, including unusual activity and CTR reports and the cross-border declarations for detecting operational cases. This should include periodic analysis of the different types of reports.

e) The LEAs should provide sufficient regular written feedback to the EFIU on disseminations, in order to enable the EFIU to have accurate knowledge about the outcomes of its disseminations and understanding about the relevance and utility of its work. Authorities should maintain detailed statistics on the use of EFIU disseminations.

f) The EFIU should revise its written policies and procedures for, at a minimum, its core operational functions (preliminary analysis, in-depth analysis and strategic analysis).

g) The EFIU should continue increasing and strengthening its human (number of analysts) and IT resources.

Immediate Outcome 7

a) Estonia should expeditiously ensure that judiciary's and LEAs' interpretation of the ML offence is aligned with the international standards and domestic legislation. This should be approached by taking steps such as (but not limited to): (i) developing formal guidelines drawing on international and domestic requirements for ML offence and good practice for investigating and prosecuting ML offence, (ii) continuing to bring prosecutions in court and appealing decisions to promote evolving jurisprudence on ML cases in line with the current criminalisation of ML and international standards, (iii) holding regular training and seminars for judges, prosecutors and investigators.

b) Estonia should prioritise ML investigation and prosecution and ensure that all sources are fully harvested for potential ML including incoming MLA requests. Parallel financial investigations should be used regularly to pursue ML. LEAs and prosecutors should maximise efforts for identifying and investigating complex types of ML with special attention to cases which involve the misuse of legal persons and CSPs and whether such persons should be prosecuted. Estonia should consider aligning its efforts to ML risk in the country.

c) Estonia should conduct a comprehensive review of applied sanctions for ML, including the parameters of its policy on plea bargaining, the nominal fines for legal persons, and most importantly the lenient practice of nearly all imprisonment sentences for ML being conditional (suspended). The authorities are encouraged (as part of plea bargain agreements and following contested

trials) to continue to push for more stringent imprisonment sentences, and where appropriate, actual imprisonment, for serious ML offences.

d) Estonia should develop the capacity to measure its own performance in ML prosecutions and convictions by fully implementing measures to develop and keep reliable, reconciled and centralised data and statistics on ML investigations, prosecutions and convictions (including information retained on the triggers for investigation, the underlying predicate offences, and other key information pertinent to risk). The authorities should regularly review this data to determine policy implications and identify the need for any corrective actions and/or application of resources.

Immediate Outcome 8

a) Estonia should enhance to a major extent its efforts to seize, confiscate and recover the proceeds of ML and predicate offences, especially those moved abroad, in line with its ML/TF risks. The results should be periodically analysed in terms of their adequacy, the consistency with risks and any challenges, actual or potential, that the authorities have faced.

b) Estonia should regularly conduct parallel financial investigations to detect the proceeds of crime and instrumentalities. Estonia should develop a manual for conducting parallel financial investigations to guide LEAs on how to trace and secure proceeds of crime especially those (i) moved abroad; and (ii) which include complex assets (such as legal persons and VAs). The LEAs shall be provided with regular training on detecting, tracing and confiscating the criminal proceeds, and instrumentalities, or property of equivalent value.

c) Estonia should ensure it has the capacity and expertise for the management of seized and confiscated legal persons and other income generating assets and new technologies and should develop adequate guidelines and deliver training to ensure effectiveness. In addition, authorities may consider setting up a centralised full-time asset management office.

d) Estonia should review the sanctioning regime related to the cross–border transportation of cash and BNI in order to ensure that sanctions are effective, proportionate and dissuasive.

e) Estonia should maintain comprehensive statistics on seizures and confiscations of property as well as for property recovered. Such statistics should be broken down by type of confiscation (instrumentalities, proceeds of crime, extended confiscation), predicate offences, amount of assets and by type of property confiscated.

f) Estonia should consider to regularly use assets sharing mechanism with foreign jurisdictions when confiscating assets with joint efforts.

154. The relevant IOs considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

3.2.1. Use of financial intelligence and other information

155. Financial intelligence along with other relevant information are gathered and used by the competent authorities to initiate and support ongoing investigations, to develop evidence and to trace criminal proceeds. Proceeds of crime are traced as a matter of policy and financial intelligence is routinely utilised for that purpose. This is done to a major extent in relation to proceeds-generating predicate offences, and to a considerably lesser extent to ML, for the reasons explained in detail under IO7. Financial intelligence plays an important role in counter-TF activities, when pursued.

156. In order to support their efforts, the competent authorities gather information, including financial intelligence, from a broad range of content-rich domestic databases including, but not limited to, the Population Register, the BR, e-Land Register, Border control information system, ETCB database, Database of detainees and probationers, Criminal Records Database, Personal identification and procedural information system, PBGB information system, and the Prosecutor's office information system. Most of these databases offer direct electronic access to the maintained information. Where access is not direct, the authorities reported having smooth request-based access to this information.

157. The authorities suggested that the ETCB database contains various important financial intelligence information including the VAT reports of legal entities' transactions above EUR 1000. This database serves as an important source for the ETCB and PBGB in performing their duties.

158. Another important source of intelligence data is the PBGB's intelligence database. It is accessed by the ETCB, the ISS and the EFIU. The system provides access to information on targets, criminal offences, evidence collected through the proceedings, including the results of surveillance, and other related data on cases in the pre-investigative and investigative phases. This database also contains information on all MLA and EIO requests handled by the PBGB. The system allows for uploading information and exchange of intelligence among the mentioned authorities. The EFIU demonstrated that it systematically uses this database for verifying information received through the OEs' reports, for foreign cooperation, and for sharing information where links are identified.

159. The EFIU database contains a wide variety of information on all the reports submitted by OEs, on reports made by other national authorities, and on foreign incoming requests. It serves as an important source of information for LEAs in pursuing their investigations. The EFIU database is not directly accessible by any of the other authorities and the information is provided on the EFIU's own initiative or upon request.

160. Information from FIs and DNFBPs is received and obtained through various arrangements for the purposes of EFIU analysis and for the operational and investigative needs of the LEAs and the PO. This information is gathered through the reporting of a variety of suspicion- and threshold-based reports filed with the EFIU by OEs, on the basis of EFIU precepts, and upon the direct request of the LEAs and the PO.

161. In order to facilitate the exchange of information between the OEs and the authorities, in 2020 Estonia launched a system that enables direct requests for information to domestic banks.

So far, 8 out of 15 banks, including the 5 largest ones, are connected to the system. Among others, information regarding the existence of an account, authorised person, BO, account balance, and a statement is regularly requested by the PBGB and the ETCB (within the limits of their rights for accessing banking secrecy information) and by the EFIU. The EFIU suggested that when they file a request, it is treated promptly, and responded to within hours, or maximum within one working day. The EFIU and competent authorities have reported extensive use of the system to request information from the private sector.

162. Among the LEAs, the ISS can request from OEs information covered by banking secrecy at any stage of analysis, even prior to the opening of a criminal proceeding. However, the PBGB, the ETCB and the PO may only access this information after the opening of a criminal proceeding. The authorities suggested that the bar for opening a criminal case is low, and that this limitation does not hinder their abilities to access banking secrecy information when needed. Before a criminal proceeding is opened, when LEAs and the PO have a suspicion of ML/TF or predicate offences, they seek the information through the EFIU. The authorities advised that, given the EFIU's extensive powers, it can request financial information on behalf of LEAs, conduct an analysis based on the information received and provide intelligence to LEAs to assist them.

163. The LEAs demonstrated that they utilise their powers for obtaining intelligence information through operational-intelligence analyses, surveillance activities, and the exchange of intelligence and other relevant information with foreign counterparts and with domestic authorities, including with the EFIU and the EFSA.

164. The LEAs demonstrated that they actively exploit their respective sources of information, though to various extents, when performing their functions, but most of the financial intelligence and other relevant information is used in relation to proceeds-generating predicate offences. Incoming MLA requests are not used systematically and have rarely triggered any ML investigation. The use of this information and intelligence for pursuing ML does not match the expectations given the risk profile of the country and the demonstrated cases where an ML investigation was not pursued due to the limitations in the system (see also IO.7).

165. As concerns the use of financial intelligence for tracing the proceeds of crime, the authorities have demonstrated that their detection capabilities are generally limited to funds and assets that reside in Estonia, whereas the risk assessments suggest that ML risks in Estonia are characterised, in particular, by the movement of funds derived from crimes committed abroad or of unknown origin through the Estonian financial system or VASPs (see also IO.8).

166. The Asset Recovery Bureau (ARB) plays an important role in detecting and securing assets. The ARB, as a part of the PBGB structure, has access to a wide range of databases. It is an active actor in investigations led not only by the PBGB but also the ETBC and the ISS. In many cases the ARB joins the investigation at an early stage. Its role is to gather information, including financial intelligence and localise all the assets directly or indirectly affiliated to the targets.

Box N°3.1 ML detected as a result of ARO actions

In November 2015 a criminal case was initiated on the basis of suspected fraud. In 2016 ARB started a parallel financial investigation to identify possible criminal assets and persons who are involved in hiding assets. Analysis of bank statements revealed suspicion of ML: in order to hide the origin of money, the suspects had transferred funds to other

companies' accounts owned and/or controlled by suspected persons. The transferred funds were used for personal purposes or cashed out. The period of ML was from September 2013 to November 2016.

In total, ARB investigated 17 persons' bank statements and other documents to find evidence for ML and criminal assets. In this case, the ARB cooperated also with the EFIU, requesting information, and obtaining also additional data. Difference between the lifestyle and the legal income was more than EUR 300 000 and ARB was able to conclude that the proceeds of a criminal nature were obtained in the amount of over EUR 375 000. ARB secured a seizure of assets (2 immovable properties) worth over EUR 266 000 in order to ensure further confiscation, concluding its investigation in June 2017.

As a result, a group of 8 persons were convicted for systematically committing fraud on a large scale and 4 members of the group were also convicted of ML on a large scale. EUR 161 830,15 was confiscated. In addition, the victim's restitution requests were fulfilled.

167. The PBGB have demonstrated that most ML investigations were triggered by intelligence and other information gathered on its own capacities, including by means of information requests to other authorities. At the same time, the PBGB acknowledged the valuable supportive role of the EFIU in providing financial intelligence both in relation to proceeds-generating offences and ML.

168. The PBGB reported that they produce annual serious and organised crime threat assessments that identify the biggest threats and choose their investigative and intelligence targets based on their impact. This is done by collecting and analysing the PBGB's own intelligence information, EFIU financial intelligence, information contained in MLA requests, information exchanged through direct cooperation with foreign counterparts, and information accessible through various domestic information databases. This was not possible to verify since these assessments were considered secret documents and were not provided to the AT. As such, the authorities did not articulate on the analysis conducted and the results achieved on-site, but provided the below described case later in the process.

Box N°3.2 Investigation arising from Annual Serious and Organised Crime Threat Assessment

In the 2020 Annual Serious and Organised Crime Threat Assessment report, the PBGB analysed MLAs and EIOs that concerned requests of bank account information to understand whether there is a correlation and connection. This information was then compared to the known information in the PBGB database and to public information, including lists of licensed entities in Estonia and company registry information about an identified CSP A that had more connections than could be reasonable. The PBGB also requested input about this CSP A and CSPs in general, from the ETCB and the EFIU.

The ETCB provided all the information it had, including its internal risk analysis of certain CSPs.

The EFIU shared its information on CSPs in general and concerning CSP A, in particular. The EFIU responded to the request and followed up with a dissemination.

The analysis of the collected data enabled launching a criminal investigation.

169. The following case demonstrates a positive example of detection and investigation of ML on the basis of financial intelligence and other information gathered by the PBGB.

Box N°3.3 Investigation initiated by PBGB - ML

In 2017, an investigation was triggered by a piece of financial intelligence from bilateral information exchange with country F regarding USD 100 received on a Local Bitcoins (LB) account of a certain Estonian citizen A. After enriching

this with financial intelligence from banks, PBGB databases and intelligence gathering operational measures it was suspected that the owner of this LB account was laundering money gained from cybercrime. Through intelligence work it was established that person A was renting a trojan malware for money and had regular customers for years – thus generating some hundreds of thousands of dollars' worth of criminal income. Person A received payments in VAs and moved the coins through mixers then received money on LB or Revolut or similar accounts that were under money-mule names. The ARO analyst identified from bank logs obtained by EIOs that person A transferred the funds to his mother's and mother-in-law's bank accounts and withdrew them from ATMs himself, confirmed with surveillance. Person A was sentenced for computer crimes, as well as ML. About EUR 100 000 worth of goods were confiscated and part of an apartment was seized. In addition, EUR 60 000 worth of debt to the Estonian Government was sentenced for already spent criminal income.

170. The ETCB has demonstrated that most of the conducted investigations were triggered by intelligence and other information gathered on its own capacity. In order to detect and investigate a crime, the ETCB systematically collects information on tax reports and payments of duties, cross-border movements of goods and financial assets and information on bank accounts and transactions carried out by taxpayers, etc. which is systematised and gathered within the ETCB electronic database.

171. The ETCB explained that its strategic target is to collect state taxes. Therefore, in most cases, the investigative efforts of the ETCB and their use of financial intelligence are focused on pursuing tax and customs crimes. The ETCB does not prioritise criminal cases simply upon suspicion of ML but for a possible positive impact on a certain field of business activity or region. In most of the presented ML cases, the ETCB plays a supportive role, by either joining the investigation team led by the PBGB, or by sharing tax crime-related information to support the ML investigation. Only rarely does the ETCB initiate an investigation into ML in relation to a tax crime, for the reasons explained under IO.7.

172. The ETCB Investigation Department reported that they prepare annual organised crime threat assessments (OCTA) about the organised criminal groups or individuals which have high potential to commit tax or customs-related crimes or drug trafficking (predicate crimes for ML). If specific information is available, then groups or individuals who are offering ML services to other groups are mentioned and ML schemes are described. Annual targets are selected from reported groups. The OCTA is shared with the Prosecutor's Office, PBGB, EFIU, ISS, Estonian Foreign Intelligence Service and the Coordination Bureau of the Government Office. This was not possible to verify since these assessments were considered secret documents and were not provided to the AT. As such, the authorities did not articulate on the analysis conducted and the results achieved on-site. Nevertheless, after the onsite the ETCB provided information on the annual key performance indicators, and the assessment of those results. The ETCB indicated that the annual mapping of the criminal threats affecting the areas of taxation and public protection, on which the targets of criminal proceedings are based, yielded a higher level of performance results than was planned.

173. Detection of criminal proceeds is a priority for the ETCB. While the volume of assets was not made available, the ETCB had demonstrated through the outcomes of implementation of its Strategic Plan for the years 2017-2020 that the ratio of criminal cases secured by arrests out of the criminal cases delivered to the OPG is up to 33%, being higher than the expected level for any given year. This indicates the use of ETCB intelligence for following the proceeds of crime and successfully securing those.

174. The below case is an example of the ETCB successfully detecting and investigating a tax fraud offense together with ML, using financial intelligence, detecting and securing the criminal proceeds.

Box N°3.4 Investigation initiated by the ETCB – Tax fraud and ML

Proceedings were commenced on 21.10.2016, based on the analysis of the information available in the ETCB databases (tax declarations). There were grounds to believe that person MM had been committing a tax crime by using various non-existent merchants. It was established within the proceedings that MM, assisted by HL and RL, submitted fictitious invoices, as a result of which the VAT liability was concealed, causing a damage to the state economy. According to information collected during the proceedings (tax declarations, bank accounts, ATM statements analysed), MM submitted false invoices on behalf of non-existent merchants from June 2016 to March 2017, on the basis of which bank transfers were made to the accounts of non-existent merchants, managed by MM; from those accounts, according to the instructions by MM, the cash was withdrawn from ATMs and delivered back to MM.

During the investigation, a total tax damage of EUR 212 438 was identified, and EUR 201 485 was seized (money on companies' bank accounts) for the fulfilment of tax obligations.

Within the proceedings, important evidence came up in the VAT returns and bank accounts.

Suspicion of ML was filed with the GPO. As a result, MM was convicted and sentenced for the predicate offence to 2 years of imprisonment, and for ML to 1 year of imprisonment. As an aggregate punishment of 2 years served concurrently, the sentence was left unenforced conditionally. Assets (a bank account and a vehicle) were confiscated for a total amount of EUR 30 313.

175. The ISS is an investigative body for high-end corruption and related ML. The ISS actively uses various procedural methods, including real-time surveillance operations for gathering information. This is further accompanied by the supportive financial intelligence provided by the EFIU in relation to financial assets.

Box N°3.5 Investigation initiated by the ISS - Bribery and ML agreement

In 2017, the ISS conducted an intelligence-led investigation. As the predicate offence, aiding and abetting accepting a bribe was committed. By means of criminal proceeds, concealment activities were performed within a period of ten years. In this case, a significant amount of time was spent on parallel financial investigations, as different companies, bogus transactions and intermediaries were used for layering and integrating proceeds of crime, i.e., conducting ML. Although the companies were engaged in legitimate business, the essence of such companies was to conceal and reverse the proceeds of crime in such a way that the proceeds of the bribe-takers could not be established without comparing the agreements and financial data. The EFIU's help was also used in those activities, and it was also invited to the operational meetings of the LEAs. The contribution of the accused persons in ML laid in fact that they worked out a plan on how to arrange sending the amounts received as a bribe to the company, which was used to prepare sham contracts and invoices to carry out the sham transactions. Object of ML was EUR 446 596,63.

As a result, the first natural person was sentenced for aiding and abetting accepting a bribe to 2 years of imprisonment, and for ML to 2 years and 7 months of imprisonment. The aggregate punishment was 2 years and 7 months of conditional imprisonment. The second natural person was sentenced for aiding and abetting accepting a bribe - to 3 years of imprisonment and for ML to 4 years of imprisonment. The aggregate punishment was 4 years of conditional imprisonment.

176. As concerns the country's efforts on TF, the main authority responsible for identifying and investigating terrorism-related offences, including TF, is the ISS. The main focus of the ISS appeared to be on intelligence-based investigations. When describing these cases, the ISS demonstrated that they use various sources of information, including information from the EFIU,

with a focus on checking transactions for funds that could be linked to persons under consideration. Over the period under consideration there were 51 intelligence investigations conducted by the ISS, of which 5 criminal investigations were initiated. One case resulted in a conviction. Features of these cases indicate the authorities' skills and knowledge in using financial intelligence in dealing with TF offences. There are nevertheless doubts around the level of awareness about the TF risks and hence the adequacy of the use of intelligence regarding whether they are aligned with those risks (see also IO.1 and IO.9).

3.2.2. STRs received and requested by competent authorities

177. The EFIU is the central authority for the receipt of 7 different types of reports from obliged entities: suspicious transaction reports (STRs), terrorism financing reports (TFRs), unusual transaction reports (UTRs), unusual activity reports (UARs), unusual activity reports relating to terrorism financing (TF_UARs), cash transaction reports (CTRs), and international sanctions reports (ISRs)[127]. In addition to this, the EFIU is also the recipient of declarations on the cross-border transportation of cash and bearer negotiable instruments (BNIs), submitted on a monthly basis by the ETCB.

Table N°3.1: Number of reports filed by OEs, per type of report

Report type	2015	2016	2017	2018	2019	2020	2021	Total
STR	529	987	1 484	1 384	1 971	2 918	12 121[128]	**21 394**
UAR	1 621	931	785	829	1 439	2 498[129]	1 098	**9 201**
UTR	1 102	637	500	710	744	609	844	**5 146**
TR_UAR	2 031	567	477	184	367	229	299	**4 154**
TFR	2	0	0	2	3	10[130]	4	**21**
ISR	16	12	31	13	89	51	99	**311**
CTR	2 451	1 894	1 573	1 242	924	1 229	1 364	**10 677**
Total	**7 752**	**5 028**	**4 850**	**4 364**	**5 537**	**7 544**	**15 829**	**50 904**

178. The authorities see advantages in having this wide array of reports. Being a transit country, it is hard to instantly detect ML suspicion, and those various types of reports enrich the EFIU's database, allowing over time the observation and detection of schemes of laundering proceeds of crime. While sharing the concern of the country in respect to the difficulty for a transit country to detect ML cases and the necessity in having a wide range of information, the AT has observed a number of weaknesses in the system, which raise concerns about the value provided by these various reports, taking into consideration the quantity and the quality of the reporting by the OEs which is impacted by various factors, as described below.

[127] Reporting of ISRs is analysed under IO.10 and IO.11
[128] The figures increased in 2021 as one service provider that provides correspondent banking services filed 10 000 fraud reports.
[129] The increase in the number of reports is due to the off-boarding of customers by two banks: Bank 1 submitted 1 035 UARs in 2020 vs. 21 in 2021 and Bank 2 submitted 549 UARs in 2020 vs. 159 UARs in 2021).
[130] Out of the 10 TFRs, 3 were submitted by VASPs, 2 by notaries, 2 by banks and 3 by the ISS. There was no common pattern of change in the environment to affect the reporting. Of the three submitted by the ISS, one was archived, one was analysed in-depth, and one was included in an ongoing case under in-depth analysis.

179. The OEs are provided with guidelines issued by the EFIU. These aim to provide instructions for OEs for the fulfilment of their reporting requirements and contain a non-exhaustive list of indicators for each category of report so as to differentiate one category from another. However, an analysis of these guidelines shows their quality to be questionable because: (a) the criteria for categorising a report as an STR entail a high level of certainty that ML or TF has occurred, the bar being close to a level of actual knowledge of the commission of a crime; (b) some of the indicators listed under UARs or UTRs clearly relate to suspicion, though they do not give rise to the submission of an STR, and (c) many of the indicators included in the guidelines are found in more than one reporting category. These deficiencies have implications on both the OEs' performance and the application by the EFIU of its prioritisation mechanisms, as described below.

180. The OEs confirmed that the application of the indicators eases the reporting process, but also creates confusion as to which category of report shall be filed to the EFIU. The majority of the OEs, including the material ones, described that, when filing the report, they are not in all circumstances doing so by first deciding on the category of the report, but rather adjusting to the indicators. Another issue is that the OEs tend to favour filing non-STR reports as those do not require the OE to temporarily refrain from conducting a transaction before they have the EFIU's feedback. This, on the one hand, does not interfere with their business activities even where suspicions are present and, on the other hand, provides them with a sense of comfort in that they believe to be demonstrating to the supervisory authorities a proper implementation of the reporting requirements by adhering closely to the provided indicators.

181. The figures provided in the Table below suggest an underreporting of STRs. Indeed, despite the fact that the STR category exists to capture operations that should be suspended, nearly a quarter of the suspension orders issued by the EFIU between 2019 and 2021[131] were borne out of UTRs and UARs, suggesting that OEs are in many cases submitting a wrong category of report and are underreporting STRs. This issue is also relevant in terms of the success of the LEAs in detecting and tracing criminal proceeds, which, as described above, is an issue when the proceeds leave Estonia.

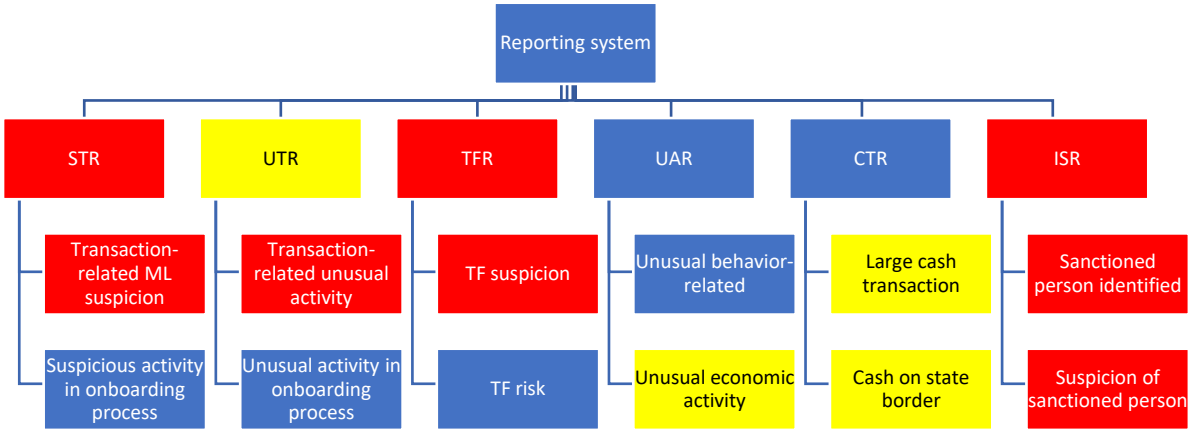
Table N°3.2. Breakdown of reports involving suspensions, by type of report (2019-2021)

STR	UAR	UTR	TFR	TR_UAR	CTR
127	18	42	0	1	55
52%	7%	17%	0%	0%	23%

182. This issue of reporting has also the following practical consequences since the EFIU prioritises reports based on the type of report, with STRs being given higher priority. Therefore, a report that should have been sent as an STR but was categorised instead as a UTR, automatically receives a lower priority level. This is an important issue for a transit country like Estonia, where illicit funds remain in the jurisdiction for only a limited time and where time is consequently of the essence. As such, it is highly important that OEs be optimally positioned to correctly indicate the type of report, including by receiving clearer instructions and guidelines and through additional training.

[131] Figures are available only for the years 2019-2021.

Figure N° 3.1.: EFIU report prioritisation system



Background colours:
Red- High priority reports
Yellow- Medium priority reports
Blue- Low priority reports

183. In terms of overall reporting by sector, as demonstrated in IO.4, most reports come from the banking sector, which files around 70% of reports, followed by VASPs at 12% and money remittance providers at around 10%. The remaining 19 sectors together account for only 12% of reports. While overarching issues with non-reporting in the sectors exist, in general, the share of reports submitted by banks is reflective of the risk and materiality of the sector, but the same cannot be said about the other important sectors, such as VASPs, CSPs and investment sectors.

184. While reporting by VASPs has increased in recent years, nearly 75% of the VASPs actively operating in Estonia did not report a transaction to the EFIU in 2021. The reports that were submitted were of very low quality, raising doubts on the part of the EFIU about the ability of those entities to correctly identify suspicious transactions[132].The authorities have advised that they have made efforts to increase reporting by those sectors, but these efforts are not yet enough.

185. At the entity-specific level, three major banks submitted retrospective reports during the assessment period, with one bank alone submitting 2 100 reports in relation to activities that occurred several years prior, and only after the related criminal activity was made public. A few banks, although being of a relatively smaller materiality and of moderate and low risk, filed no STRs at all, some, systematically, over the years.

186. Moreover, the reports received do not adequately reflect the most prevalent ML predicate offenses affecting Estonia, i.e., fraud, tax offenses, narcotics-related offenses, and embezzlement. For the two years 2020-2021, an average of 3% of all reports related to either tax offenses, narcotics-related offenses or embezzlement. While the number of reports relating to fraud were much more in line with the country's profile, those relating to VASPs were on average quite low, especially given the risk level associated with the activities of VASPs.

[132] EFIU Report "The Risks Related to Virtual Asset Service Providers in Estonia" from January 2022, page 20.

Table N°3.3: OE's reports received by the EFIU, per main crimes[133]

	2020		2021	
Crime	**No. reports**	**% Share**	**No. reports**	**% Share**
Fraud	1 665	23%	10 045*	63%
Cryptocurrency/VASP-related	238	3.2%	3 721	24%
Tax Offenses	170	2.3%	171	1.1%
Narcotics-related Offenses	126	1.7%	65	0.4%
Embezzlement	23	0.3%	34	0.2%

* Of which 10 000 from one bank. Excluding this figure, the number of reports falls to 45 and the share to about 0,44%.

187. Low quality reporting is a long-standing issue. This problem was recognised by the EFIU in 2016, when it made efforts to focus the attention of FIs on more precise and content-rich reports instead of on the quantity of reports submitted. While this effort has been ongoing, the phenomenon still exists and warrants further attention.

188. The quality of reporting is partly demonstrated in the table below which reflects, in an aggregated manner, the use of the various types of reports filed by all OEs for EFIU in-depth analysis and dissemination. This further supports the observation that the reports filed by OEs are generally not high-value reports from a financial intelligence standpoint.

Table N°3.4: Number of reports received, analysed in-depth, and subsequently disseminated

	2015					2016					2017					2018				
Types of reports	Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated	
	N°	N°	%	N°	%	N°	N°	%	N°	%	N°	N°	%	N°	%	N°	N°	%	N°	%
STR	529	137	**26**			987	176	**18**			1484	239	**16**			1384	337	**24**		
UAR	1621	367	**23**	336	**10**	931	219	**24**	145	**7**	785	186	**24**	177	**6**	829	159	**19**	239	**8**
UTR	1102	157	**14**			637	91	**14**			500	134	**27**			710	217	**31**		
TR_UAR	2031	25	**1**	26	**1**	567	16	**3**	15	**1**	477	15	**3**	5	**1**	184	3	**2**	4	**2**
TFR	2	2	**100**			0	0	**0**			0	0	**0**			2	0	**0**		
CTR	2451	845	**34**	287	**12**	1894	533	**28**	260	**14**	1573	491	**31**	206	**13**	1242	207	**17**	154	**12**

	2019					2020					2021					2015-2021				
Types of reports	Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated		Received	Analysed		Dissemi-nated	
	N°	N°	%	N°	%	N°	N°	%	N°	%	N°	N°	%	N°	%	N°	N°	%	N°	%
STR	1971	415	**21**	398	**10**	2918	276	**9**	127	**4**	12121[134]	352	**3**	174	**1**	21394	1932	**9**	1,628	**8**
UAR	1439	306	**21**			2498	446	**18**	239	**10**	1098	121	**11**	34	**3**	9201	1804	**20**	273	**3**
UTR	744	184	**25**			609	96	**16**	54	**9**	844	56	**7**	29	**3**	5146	935	**18**	83	**2**
TR_UAR	367	27	**7**	28	**8**	229	5	**2**	229	**100**	299	5	**2**	299	**100**	4154	96	**2**	607	**15**
TFR	3	1	**33**			10	4	**40**	7	**70**	4	1	**25**	4	**100**	21	7	**33**		
CTR	924	301	**33**	243	**26**	1229	923	**75**	566	**46**	1364	976	**72**	4	**0.2**	10677	4276	**40**	1716	**16**

[133] Statistics available for 2020-2021.
[134] The figures for STRs increased in 2021 as one service provider that provides correspondent banking services filed 10 000 fraud reports.

189. The EFIU advised that many of the reports not submitted for in-depth analysis are nonetheless shared with LEAs via direct disseminations to the PBGB database, as presented in the table below. The types of the reports are not detailed. While this is a positive practice of cooperation between the EFIU and LEAs, wherein the EFIU aligns its efforts to the needs of LEAs, there is no indication regarding the support that these direct disseminations provide to LEAs.

Table N°3.5: Number of reports disseminated to PBGB database[135]

Year	2017	2018	2019	2020	2021
Reports disseminated	234	432	752	664	103

190. When considering the reporting of TR_UARs, the authorities explained the high number of received reports by the fact that, in the past, reports were based only on a link with a high-risk jurisdiction. Since 2019, the OEs are required to submit a report only when, in addition to a link with a high-risk country, there are also one or more other indicators[136] in the presence of TF-related considerations. Nevertheless, except for the year 2019, there has been no change in the trend of usability of those reports for in-depth analysis. While in 2019 about 7% of reports were analysed in-depth, in the years 2020-2021 that share fell to only 2% of reports. Since 2020, the EFIU is in the practice of sharing all TF reports with the ISS, to serve as additional information for their intelligence purposes.

191. Estonia has chosen to establish among other categories, also cash threshold reporting. The threshold set for CTR reporting is EUR 32 000. The reports filed are used for the purposes of filling the EFIU database, and thus in carrying out their analyses when links with those transactions are identified in the scope of the case analysis. Indeed, as seen in Table N°3.4, many CTRs formed part of the in-depth analysis process and were subsequently disseminated to LEAs, suggesting that they are assisting the EFIU in performing its functions. This demonstrates that these are a valuable source of operational information for the EFIU, and therefore, bearing in mind the risk profile of Estonia, there might be grounds for reducing the threshold and expanding the reporting obligation also to credit institutions in the circumstances where those are exempted by the legislation, thus allowing the EFIU to have a wider picture and a higher detection capability of ML/TF schemes.

192. The EFIU provides operational feedback on individual STRs with reporting deficiencies, annual feedback to OEs or sectors, and training programmes.

193. The authorities suggested that between 2015-2018, operational feedback regarding reporting deficiencies was given informally via phone to OEs. This also included clarification regarding the MLTFPA, and on AML/CFT measures in general. From 2019, the preliminary analysis group began providing written feedback via e-mail. Starting in 2020, the EFIU began providing annual feedback reports to market participants. Feedback reports include information on trends, typologies, and the quality of reporting. The EFIU provides an analysis on ML/TF typologies in its annual reports and in certain strategic analysis products. This demonstrates a positive practice and evolving progress in reaching out to the private sector with a view towards enhancing the quality and risk-relevance of the reports.

[135] Statistics is available for 2017-2021.
[136] "Guidelines on the characteristics of suspicious transactions" p. 20-21

194. Over the entirety of the review period, the feedback provided by the EFIU has been focused mainly on banks, the largest reporting sector. While the banking sector acknowledged the receipt of valuable feedback from the EFIU, including in the form of meetings, which is a recent practice, the VASP sector appeared to be more sceptical, stressing that a more tailored approach should be taken that takes into account the specificities of the products and services they provide (see IO.4). In addition, CSPs, PSPs, fund management companies and casinos (using foreign country guidelines to support their work) also stressed that almost no feedback was received from the EFIU and that they are in need of more guidelines and feedback from the authorities.

195. The EFIU receives incoming and outgoing cross-border declarations on the transportation of cash and BNIs, and information on undeclared cash and BNIs and false declarations from the ETCB, on a monthly basis. The EFIU advised that these reports have served as an additional source of information when examining a case. The EFIU has advised that it uses these reports for ongoing analyses or for conducting a strategic analysis for detecting ML/TF trends and patterns, though examples of such analyses were not provided. The ETCB had presented a case example where, on the basis of a report filed to the EFIU as a result of detention a passenger car with cash, a criminal case was initiated with the supportive input from the EFIU (see IO.8).

3.2.3. Operational needs supported by FIU analysis and dissemination

196. The EFIU was established in 1999 as an independent structural unit of the PBGB, with strong features of a police-type FIU. With the restructuring that occurred in January 2021, the EFIU became an administrative-type FIU, turning into a government agency under the jurisdiction of the MoF.

197. When it was in the PBGB, the EFIU was part of the NCP and was treated as one of the bureaus within this structure. The legislation required that the PBGB provide the EFIU with adequate resourcing (including human and IT resources). In practice, however, this was not ensured at a level that matched both the workload and the demand for advancing the utilised technology.

198. Since the structural change in 2021, the head of the EFIU is now responsible for preparing the budget proposal and for submitting it for approval to the Minister of Finance and then Parliament. Since its transition from the PBGB, the EFIU's budget has increased considerably.

199. In terms of staffing, the majority of the EFIU's staff was retained following the structural change, thereby alleviating concerns regarding the retention of the EFIU's institutional memory. As regards the staffing level, the EFIU has demonstrated progress and commitment in increasing their human resources over the years, including by now offering competitive salaries.

200. While such progress is recognised and appreciated, it cannot be ignored that the EFIU was critically understaffed for almost the entirety of the assessment period. The case analysis department, which includes the preliminary analysis, in-depth analysis, and international cooperation groups, operated with around 2-4 analysts per group during most of the assessment period (that number was lower at the start of the period, and slightly higher by the on-site visit). With an inflow of reports that ranged from 3 000 to 6 000 per year (peaking to 14 000 in 2021), and with all reports being submitted for preliminary analysis, a function which was handled by 2 analysts for most of the assessment period, the EFIU has not been equipped with the resources

necessary to meet its operational demands. The structural change to the EFIU and the recent increase in staffing levels should help to address this issue, with further benefits being expected from the additional hires the EFIU intends to make to fill the vacancies present in this department as at the on-site.

201. The strategic analysis function similarly suffered from critical understaffing. Over the last three years, however, the EFIU has increased the staff in this area as well, though a number of positions remained to be filled as at the end of the on-site. This increase in the number of strategic analysts is reflective of the expanding attention of the EFIU to this function.

202. The EFIU uses an electronic database to receive, register and process STRs and to process national and international information requests. It is the main tool used by the EFIU's analysts. It has an integrated risk scoring module for prioritising incoming reports based on meta-data information fields (a separate, manual scoring module is used to decide whether a report should be sent for in-depth analysis), and it makes connections between information included in the report and the information already existing in the database. It also includes a transaction registry and has a built-in mass query solution that provides access to several public and LEA databases. The EFIU also uses off-the-shelf analytical tools to analyse large quantities of information and has its own document management system. The EFIU uses an excel file for case monitoring purposes. The authorities suggested that these technological solutions greatly support the performance of their operational functions, and they are working on strengthening them further.

203. The EFIU has some documented procedures in place for the three working groups performing analysis: preliminary analysis, international cooperation and in-depth analysis. Specifically, the Code of Conduct for the FIU's Analytical Division covers the sources of information that must be accessed and those that are discretional, as well as the grounds for submitting a case for in-depth analysis. According to the procedures, the sources that must always be consulted are limited to the EFIU's internal database, the PBGB database, and, in the case of foreign entities, internet search engines. Other information sources, such as national registers, are left to the discretion of the analyst. Indeed, many of the important steps in the preliminary analysis process are left to the discretion of the analyst, including, in part, the decision to submit a case for in-depth analysis. The grounds for exercising discretion in deciding to submit a case for in-depth analysis include "general work schedules" and "organisation of work at the EFIU", this raising concerns that the decision to submit a case for further review is not based on the merits of the case, but rather on the workload of the in-depth analysis group. In sum, as also further demonstrated in the analysis below, the procedures do not provide a comprehensive approach to analysing reports and do little to ensure the rigour of the EFIU's analytical assessments. The EFIU has advised that it is in the process of revising these procedures, a process that should yield positive benefits.

204. Turning to the practice, the operational analysis of reports, all reports are first processed by the preliminary analysis group, which is tasked with prioritising reports and with carrying out an initial information mapping and analysis. A two-step process is used to prioritise the reports: automatic, performed directly by the database, and manual, carried out by the analyst. This serves as a basis for determining whether the report is to be archived, submitted for in-depth analysis, or disseminated to LEAs or other competent authority without in-depth analysis (including by entering information directly into the PBGB's database). Until October 2021, when an excel file

was developed for this purpose, there was no formal scoring system in place for analysts to use to make such determinations. On average, the preliminary analysis group spends 17 minutes analysing a report. The EFIU maintains that this time is sufficient given the features of its database.

205. The preliminary analysis group essentially serves as a gatekeeper for the reports received by the EFIU and determines the life cycle of every report. As demonstrated in Table N°3.4, only an average of 9% of STRs, 33% of TFRs and up to 20% of UARs and UTRs are submitted for in-depth analysis, and, consequently, result in the possible production of EFIU intelligence. While the quality of the reports received certainly plays an important role in explaining that percentage, it also likely captures shortcomings in the preliminary analysis function to identify all the reports that should be analysed further, given the shortcomings in the procedures framing the working practices, reliance on mental checklists (until October 2021) and verbal instructions, the limited human resources and the practice of automatic submission of reports to the PBGB when there is a match with their database.

206. The international cooperation group also forms the part of the preliminary analysis process, with a competence for analysing all foreign cooperation requests. When a request is found to be linked to an existing case, the international co-operation group assesses whether the new information is significant, and if so, sends it to the in-depth analysis group for further elaboration. This practice, nevertheless, is considered questionable, as the original analyst is best positioned to determine whether such information, which on its surface may not seem notable, is in fact significant to the existing case.

207. When a case is submitted for in-depth analysis, the case is put together as a whole. This part of the process produces most of the EFIU's intelligence (as the preliminary analysis function primarily serves as a filter). At this stage, a wide use of available information, data obtainable by request, including from the OEs and foreign counterparts is gathered for the performance of the full-scope analysis. The analysis ends with a summary, which forms the basis for a dissemination in case the suspicion of ML or TF is determined. As discussed in more detail below, these disseminations, representing most of the EFIU's intelligence products, have focused more on providing support to LEA investigations and cases than on detecting new targets.

208. The EFIU suggested that it does not have a backlog of cases, as on average, in-depth analysis takes 30 days, both for urgent and non-urgent cases, and the group handles about 100 cases per year. While this is typically considered a positive aspect, this reinforces the doubts regarding whether reports that deserve to be analysed in-depth are in fact being captured and forwarded for further review.

209. With regard to disseminations on TF matters, the EFIU has stated that it engages the ISS at the earliest possible time, immediately sharing the received reports with the ISS before conducting its own analysis. Those are first checked regarding the need to take suspension measures. In the case of international links, the expert will request additional information from the relevant foreign FIUs. After analysing all the collected materials and finding suspicious circumstances, the expert compiles the analytical product for dissemination to the ISS. An in-depth case file is always opened with regard to TFRs or in cases when the ISS requests information from the EFIU in relation to an on-going intelligence or criminal investigation. The in-depth analyst follows the same procedure as described above.

210. However, the statistics demonstrate that two thirds of the TFRs were not analysed in-depth by the EFIU, contrary to the EFIU's stated policies in this regard (13 out of 21 did not undergo in-depth analysis). Although TFRs are forwarded immediately to the ISS, this should not relieve the EFIU of its role in the analysing of TF and forming financial intelligence.

211. There have been instances were EFIU disseminations resulted in the opening of an investigation by the ISS. The ISS also indicated that they make use of EFIU disseminations also for their intelligence purposes. (see IO.9)

212. As a part of its case analysis the EFIU practices in-person meetings with persons whose funds or assets have been suspended by the EFIU for the purposes of ascertaining whether the funds or assets are legitimate and should be released from suspension. This is not a typical *modus operandi* for an FIU. In the view of the AT this practice of gathering information by the EFIU raises concerns since this *de facto* reveals that the OE filed a report on its customer, and risks the loss of opportunities to detect a larger picture – the criminal scheme and the linked transactions or persons and enable detection of the potential ML. This is a long-standing practice, which was also criticised in the scope of the MONEYVAL reports under the previous rounds of assessments, but no steps were taken by the country in this regard so far.

213. The EFIU divides its disseminations into three categories: crime reports, which are filed when the EFIU identifies elements of a crime during its analysis, spontaneous disseminations, which are submitted upon the initiative of the EFIU for intelligence purposes or to add to an existing criminal case and replies to information requests made by LEA during an ongoing criminal procedure. These represent the work of the EFIU in disseminating financial intelligence.

214. The table below details the types of EFIU disseminations. Information provided by the EFIU and the LEAs demonstrate that the crime reports and spontaneous disseminations are the reports that contain both the instances where the EFIU has detected the suspicious activity on its own, and the instances where it is following the LEA's lead. The latter situation includes when, in co-operation with the LEAs, the EFIU discovers a new dimension in an on-going case, which was not known to the investigative body yet. By way of example, PBGB statistics provided for 2021 on the use of EFIU crime reports demonstrates that, out of 17 crime reports, proceedings were commenced with respect to 8 crime reports, no proceedings were commenced on the basis of 5 crime reports and proceedings already existed for the same case with respect to 4 crime reports. One should note also that the EFIU files "crime reports" not only when it detects suspicion of ML/TF or associated proceeds generating crimes, but also when it detects unlicensed activity, and the provision of false information at the licencing stage (e.g., VASPs)[137]. The other types of disseminations, namely the spontaneous disseminations related to an ongoing investigation and the responses to requests are the types of disseminations where the EFIU follows the LEAs investigative needs.

215. In addition to these disseminations, as presented in Table N°3.5, the EFIU shares with LEAs reports received from the OEs via direct disseminations to the PBGB database, where a match is identified. While this is another positive practice of co-operation between the EFIU and LEAs,

[137] EFIU Report "The Risks Related to Virtual Asset Service Providers in Estonia" from January 2022, p.20.

those types of disseminations suggest the sharing of information, which was not enriched by the EFIU's analytical input (in-depth analysis).

216. On the basis of the above presented explanations and the statistics provided in Table N°3.6 Estonia should be commended for the demonstrated practice of co-ordination and co-operation between the EFIU and LEAs and the EFIU's efforts to meet the operational needs of the LEAs.

217. On the other hand, nevertheless, it is observed that there is a moderate improvement required in the EFIU's capacities and working practices for reinforcing its proactive approach in the detection of cases versus to the current reactive approach which is heavily reliant on the LEA's lead. This is a priority matter in the context of Estonia, as the EFIU is best placed to observe and detect the movement of illicit funds through the Estonian financial and non-financial sectors on the basis of the wide variety of reports filed by the OEs and other available information. In contrast, the LEAs (except for the ISS) can analyse only publicly available information, own intelligence and foreign country requests or information to detect crime.

Table N°3.6: EFIU disseminations to LEAs

	2015					2016					2017					2018			
	PBGB	ISS	ETCB	PGO	**Total**	PBGB	ISS	ETCB	PGO	**Total**	PBGB	ISS	ETCB	PGO	**Total**	PBGB	ISS	ETCB	PGO
Crime report	1	1	0	12	14	0	1	1	10	**12**	5	0	0	8	**13**	50	1	0	0
Spontaneous dissemination	37	1	31	1	70	14	0	11	1	**26**	9	0	4	0	**13**	94	40	11	0
Spontaneous dissemination related to an ongoing investigation	34	0	8	3	43	27	0	16	6	**49**	48	0	7	4	**59**	81	0	3	11
Reply to a request (ongoing investigations)	36	2	3	1	42	56	1	11	1	**69**	103	4	21	9	**137**	42	0	9	1
Total	108	4	42	17	169	97	2	39	18	**156**	165	4	32	21	**222**	267	41	23	12

	2019					2020					2021			
	PBGB	ISS	ETCB	PGO	**Total**	PBGB	ISS	ETCB	PGO	**Total**	PBGB	ISS	ETCB	**Total**
Crime report	16	0	0	7	**23**	6	0	0	0	**6**	17	1	0	**18**
Spontaneous dissemination	81	74	15	4	**174**	116	68	23	2	**209**	53	37	4	**94**
Spontaneous dissemination related to an ongoing investigation	116	0	2	13	**131**	74	0	4	0	**78**	29	0	0	**29**
Response to a request (ongoing investigations)	64	0	3	0	**67**	146	0	21	1	**168**	134	2	9	**145**
Total	277	74	20	24	**395**	342	68	48	3	**461**	233	40	13	**286**

218. No regular statistics are maintained in Estonia to analyse the outcome of the EFIU disseminations for all the period under observation. The PBGB has presented some data for 2021 on the use of EFIU criminal reports (see analysis above), spontaneous disseminations (indicating the recipient units within the PBGB, but not indicating the outcomes), spontaneous

disseminations related to on-going investigations (indicating the criminal matters) and responses to requests (indicating the criminal matters). On the basis of this information, it was observed that, in the majority of instances, the EFIU information is used to initiate proceedings into the ML predicate offences – fraud being the most prevalent one.

219. While no comprehensive statistics are available on the input of the EFIU into detection of ML cases, the PBGB also retrieved indicative figures on the cases commenced with EFIU supportive information and crime reports (see IO7). An analysis of the provided information and the provided case examples demonstrates that the EFIU had input into some relatively larger and complex ML cases, such as the "Butterfly" case – developed on the basis of a foreign FIU incoming request and EFSA report, formally initiated on the basis of an EFIU dissemination; "Bank D" – developed on the basis of the joint efforts of the authorities and formally initiated on the basis of an EFIU dissemination; "Bank S" – initiated on the basis of the EFSA's dissemination, with the EFIU providing supporting information; "Tirmaste and others" - initiated by the LEAs, with the EFIU providing supporting information; and "Hirvi" - initiated by the LEAs, with the EFIU providing supporting information.

220. In addition, the following are examples of some LEA investigations triggered on the basis of EFIU criminal reports.

Box N°3.6 PBGB investigation of ML (crowd-funding platform)

initiated on the basis of EFIU dissemination

Estonian company X, manager of a crowd-funding platform, transferred millions of euros to its account in foreign country A. The credit institution servicing the accounts of company X suspected that the latter was not using the funds it received for their intended purpose and asked for additional information. Once the company X refused to provide it, the credit institution blocked the account of company X account and submitted an urgent report to the EFIU in 2020.

The EFIU analysed the report and, as a result of its preliminary analysis, found negative background information on a person related to the actual beneficiary of company X. The EFIU imposed a restriction on the account of company X and subsequently asked all Estonian credit institutions for information related to company X, questioned the authorised representative of company X and requested information from the FIU of country A.

The authorised representative of company X was not able to explain to the EFIU the substance or legality of the company's payment behaviour, nor did he provide any additional documents or evidence regarding the origin of the money, the intended nature of the transactions or the company's activities. It was suspected that the platform advertised some fictitious projects. The account of company X was suspended for an additional 60 days. The company X was requested to provide additional information on its investment projects and the member of the management board was called to provide explanations.

The EFIU submitted a criminal report to the PBGB, followed by several disseminations thereafter to supplement the criminal case. During the additional analysis, it emerged that the member of the management board of company X was a straw man, and that the actual beneficiary of the company was a citizen of country B. The EFIU also cooperated with the relevant foreign FIUs and requested for restriction of funds in those jurisdictions. During the court proceedings funds were seized in Estonia and in one foreign jurisdiction.

Criminal proceedings are ongoing.

221. The EFIU also disseminates information to Estonian supervisors. The case described below resulted in the suspension of around EUR 1.2 million, a notification to the EFIU's Supervisory

Department and a dissemination to the PBGB where a criminal investigation was launched. Similar exchanges of information have also taken place with the EFSA.

Box N°3.7 PBGB investigation initiated on the basis of EFIU dissemination

In the recent year the EFIU received an STR from the licensed VASP. The VASP's main suspicion was that two accounts were opened based on forged documents (the passports had signs of counterfeiting, the client had presented two different passports with two different faces, etc.).

The VASP also noticed activity that suggested that one of the accounts was being misused. Moreover, there was adverse information on the entity that used the account (regarding a Ponzi scheme). The VASP suspended the assets and reported the matter to the EFIU.

The EFIU detected that the report was of a very poor quality: (i) the origin of the suspicious assets was not detected; (ii) the obligation to understand the client relationship was not applied; (iii) the persons with the forged documents were on-boarded; (iv) the VASP was engaged in defensive reporting; (v) an urgent report was not submitted; (vi) the VASP did not provide timely the additional information to the EFIU; (vii) a high-risk-country client was on-boarded without conducting EDD; (viii) the VASP did not have the capacity to analyse the cryptocurrency that it operates with, etc. The cooperation with the EFIU was poor. The EFIU gathered additional information from the VASP in order to restrict the suspected funds and imposed suspension for around EUR 1.2 million.

The EFIU's Supervision Department immediately initiated an on-site inspection. The EFIU planned to withdraw the license, but the VASP surrendered its license itself.

The analysis and the detected shortcomings of the VASP were disseminated to the PBGB and a criminal investigation was launched into fraud and ML. The funds were secured through the EFIU asset suspension mechanism.

222. The following are examples of the support provided by the EFIU to LEAs in ML investigations.

Box N°3.8 ETCB investigation of ML supported by the EFIU

In January 2016, the ETCB submitted a request to the EFIU regarding a group of persons involved in organising tax crimes (invoice factory). The ETCB also had a suspicion of ML so they contacted the EFIU. The EFIU had some pieces of information about subjects of the request and disseminated the information to the ETCB. In a later stage, the EFIU discovered that some of the persons were still active (performing cash withdrawals), and continued to analyse the information (existing information, requested additional information from OEs and foreign FIUs) and disseminated the relevant information to the ETCB.

During the criminal proceedings, a criminal organisation of at least 6 members was identified, which organised the commission of tax crimes in two foreign countries during 2015-2016, causing damage of approximately EUR 9.5 million. The group also laundered criminal funds from tax crimes.

As a result, 7 persons were convicted (creating an organised crime group and LM). The punishments issued were for 4 years of imprisonment (conditional) for ML and 5 years (conditional) for creating an organised crime group.

The EFIU's contribution consisted of 1.5 years of co-operation, which included 4 requests from the ETCB, 17 disseminations to the ETCB and 6 requests to foreign FIUs.

Box N°3.9 ISS investigation of ML supported by the EFIU

In 2020 the ISS initiated an investigation into corruption and ML. The EFIU was contacted in the early stages of the criminal investigation and was included in the meetings regarding the case and later provided additional financial

intelligence. The EFIU's connection to the case was after the criminal proceedings were initiated, but the EFIU's contribution to find additional financial intelligence was valuable to the case.

The EFIU made 3 disseminations on the criminal case (information from approximately 30 reports) and this information included the previous information about suspicious transactions of persons involved and information from the reports, which were submitted after the disclosure of the case.

The EFIU also followed a lead regarding a development agreement in another country, suspecting an additional element of corruption. According to public sources, a PEP from a foreign country was accused of corruption and was connected to a person of interest in this case. The EFIU had a suspicion that one of the persons of interest might have been involved in the corruption case. The lead was not confirmed but created an additional value to the criminal case.

The case is still ongoing.

223. Over the entirety of the period, the strategic analysis function of the EFIU has been limited, being impacted by the absence of adequate resourcing, as described above. Indeed, this was recognised in the 2021 NRA Action Plan, where it was stated that the EFIU does not have the capacity to adequately carry out strategic analysis.

224. The EFIU had provided a list with the titles of various strategic products developed over the years, but not the substance of those, with limited exception, hence the relevance and quality of those cannot be verified and analysed within the scope of the current assessment. Exception is the publicly available material, consisting of: the EFIU's annual reports, that usefully contain an "ML schemes" section with a detailed description of the typologies on common schemes discovered by the authorities; the EFIU's annual analysis of foreign cooperation, where the private sector is helpfully advised about the criminal proceedings related to foreign crime with connections to Estonia; and the sectoral risk assessments of the NPO, CSP and VASP sectors that assist the private sector in focusing their attention for identifying suspicious activities.

225. When coming across illicit funds, the EFIU uses its powers for postponement of assets, where considered appropriate, thus supporting the LEAs' further efforts in securing the seizure and confiscation of assets. The effect of this is described in IO8.

226. When a transaction is suspended, the funds are restricted for an initial period of 30 days (which may be extended by an additional 60 days under certain circumstances). Due to the long duration of the suspension, the EFIU notifies the owner of the suspension. However, in so doing, the EFIU risks causing harm to an eventual LEA investigation by alerting the subject that he is under scrutiny at a stage of the process that often precedes the initiation of a criminal proceeding, thereby jeopardizing the detection of crime and the tracing of assets.

227. Feedback obligations vary depending on the type of communication sent by the EFIU to LEA. If the EFIU submits a "criminal report", LEAs must inform the EFIU within 10 days regarding the use made of that report, i.e., whether a criminal proceeding was initiated and, if not, the reasons for not doing so. The PBGB could only provide statistics for 2021. It was confirmed that no statistics are available for the preceding years.

228. In the case of spontaneous disseminations by the EFIU, LEAs do not have an obligation to inform the EFIU if the information was used to open a preliminary investigation. However, regular feedback obligations were introduced in the MOUs signed by the EFIU and LEAs at end of 2020. These obligations do not appear to have been fully implemented. The EFIU and LEAs stated that for now the feedback is given verbally, but a mandatory formal feedback system is in the

development process. Unlike dissemination-specific feedback, formal feedback was provided on a yearly basis in relation to general issues. Considering the importance of consistent and meaningful feedback in the cooperation mechanism more frequent formal feedback would be expected to increase the EFIU's ability to assess and improve the quality, and consequently the utility, of its work.

3.2.4. Cooperation and exchange of information/financial intelligence

229. The competent authorities demonstrated a high degree of cooperation, coordination and exchange of financial intelligence. The EFIU has signed MOUs with the PBGB, the ETCB, the PGO and the EFSA. The memoranda lay out the principles of cooperation for the exchange of information, including the confidentially of the information exchanged, and describe the specific cooperation details according to the authority's expertise. In addition to the MOUs, the EFIU has also provided information on how to submit a request to the EFIU.

230. Cooperation between the EFIU and the competent LEAs is fast and prolific. Some LEAs, such as the PBGB and the ISS, have dedicated liaison officers responsible for communicating with the EFIU. While the level of cooperation is generally quite high between the EFIU and LEAs, the EFIU's relationship with the ISS, as the responsible body for TF investigations, is largely one-directional, with the EFIU providing information to the ISS with little or no exchange from the ISS to the EFIU.

231. In addition to the exchange of information, the EFIU and the LEAs also cooperate through bilateral and multilateral meetings on specific operational matters concerning ongoing criminal cases. When the EFIU was part of the PBGB, it was sometimes included as a member of an investigation team and participated in weekly joint meetings in this regard. Weekly meetings were also held between the heads of the investigative bureaus and the head of the EFIU. This cooperation, slightly less frequently, has continued after the EFIU moved.

232. The EFIU and the PGO also have joint meetings to discuss general cooperation issues or specific case-related questions. The EFIU maintains regular communications with the PGO in relation to European Account Preservation Orders (EAPO) and any other requests to restrict funds made by a foreign FIU.

233. The EFIU also maintains close cooperation with the EFSA. This is based on a favourable environment set out in law and is further strengthened by an MoU.

234. Most of the information exchanged between the FIU and the other competent authorities is done though secure platforms. When the EFIU shares information, each document contains relevant access restrictions and specifically states that the information disseminated by the EFIU may not be used as evidence in proceedings or disclosed to third parties without the prior written consent of the EFIU. Only an official of the EFIU has access to and the right to process information in the EFIU's database. The EFIU does not make data directly available to other authorities.

235. The EFIU takes various measures to protect its information. This is ensured through the security checks of the staff. All officials of the EFIU are subject to background checks before entering service. Additional background checks are required and carried out by the ISS for EFIU officials with access to state secrets and/or classified information of foreign states.

236. The premises of the EFIU are equipped with an adequate security system preventing the unauthorised access of third parties.

IT infrastructure

237. Information provided to the AT indicated that the country deemed it essential to replace the provider of IT services and to move the IT systems following the transition. The transition was carried out, with workplace services moved to another service provider and development of IT systems staying under the previous service provider.

238. Access to the EFIU's servers is set out in a contract between the EFIU and its IT service provider. The country suggested that the EFIU has the ability to control and monitor access to its servers.

Overall conclusions on IO.6

239. Financial intelligence along with other relevant information is gathered and used by the competent authorities to initiate and support ongoing investigations, to develop evidence and to trace criminal proceeds, this mostly to pursue the ML predicate offences. In general, access to information is smooth. Estonia should be commended for the demonstrated practice of co-ordination and co-operation between the EFIU and LEAs and the EFIU's efforts to meet the operational needs of the LEAs. On the other hand, a moderate improvement is required in the EFIU's capacities and working practices in order to reinforce its proactive approach in the detection of cases and to lessen its current heavy reliance on the LEA's lead. This is a priority matter in the context of Estonia, as the EFIU is in the best position to observe and detect the movement of illicit flows by itself. This demonstrates a serious gap in the EFIU's focus and direction of its efforts. However, this potential is greatly limited, among other things, by the low quality of reporting, which includes retroactive reporting. In addition, the EFIU's practice of contacting, and gathering information directly from the person whose funds are suspended, raises some concerns and may hamper the EFIU's and LEAs' efforts in tracing proceeds and detecting ML cases and predicate offenses.

240. Taking into consideration the availability and use of intelligence and other information, and the high degree of cooperation demonstrated by the authorities in pursuing the investigations, including the recent important developments aimed at strengthening the EFIU's capacities and its performance, moderate improvements are required.

241. **Estonia is rated as having a Substantial level of effectiveness for IO.6.**

3.3. Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML identification and investigation

242. The authorities which identify and investigate ML offence are the PBGB and its subordinate offices (NCP and Police Prefectures), the ISS, and the ETCB[138]. ML is mainly investigated by the PBGB, and when ML offence relates to tax fraud or customs offences then it may be investigated by the ETCB. In certain instances, the ISS will investigate potential ML offences when high level

[138] By Regulation RT I, 12.04.2013, 4, the PBGB is confirmed to conduct investigation in all criminal offences for which the competence had not been granted to the ISS or to another investigative authority under s.212(2) (e.g., Tax and Customs Board regarding tax and customs crimes). There are other bodies which have competence to investigate criminal offences i.e., the Competition Board, the Military Police, the Environment Board as well as the Department of Prisons of the MoJ but in practice it is the PBGB, ETCB and ISS who investigate ML.

corruption appears as the predicate. The prosecutor decides whether LEAs must start a criminal investigation, or whether the prosecutor in a particular case initiates himself/herself. Whilst there are no clear written guidelines on the demarcation between the respective ML investigative jurisdictions of each agency, there is strong co-operation among authorities; some of this is ad hoc and some is governed by Memoranda of Understanding and there is no suggestion of any difficulty in determining which agency is better placed to take on an ML investigation. Furthermore, the Estonian authorities appear (overall) to be reasonably equipped to identify and investigate ML, with some areas that could be assisted by additional resources. All the LEAs, judiciary and prosecutors undertake ML–related training.

243. The authorities have a range of special investigative measures available to them and they use these powers regularly in ML investigations. Limited statistics were available but case examples of the regular use of such measures have been presented. The LEAs also have direct access, without the need for a court order, to several databases and registers as detailed under IO.6.

244. In Estonia, different sources of information are used to trigger ML identification and investigation. The main sources from which ML is primarily identified and investigated are police reports[139] and EFIU disseminations, and to a lesser extent from financial investigations and open-source information. In the context of Estonia's risk profile, the incoming MLA requests should serve an important source for identification of ML offence. Nevertheless, in practice MLA requests are not used systematically and have rarely triggered any investigation. This raises concerns given the fact that foreign predicate offences represent the biggest ML threat in Estonia as recognised in the NRA, and as also shown by the prevalence of foreign predicate offences in ML investigations and prosecutions. On a positive note, the country had demonstrated some examples of larger ML cases, where the predicate offences have been established, inter alia, by analysing previously received MLA requests.

245. Authorities do not maintain systematised statistics on the sources of information that trigger ML investigations. However, the PBGB retrieved figures on the number of ML investigations commenced with the EFIU's disclosures or supportive information (see table 3.7).

Table N°3.7: ML investigations commenced with EFIU supportive information and reports

Year	2015	2016	2017	2018	2019	2020	2021
No.	9	4	8	26	10	2	5

246. The overall numbers are relatively low, but the examples presented by authorities demonstrate that the EFIU had an input in (even if not always triggering) larger and more complex ML cases. In 2020 the PBGB has established a new unit specialised in analyses and investigation of EFIU disseminations.

247. Estonia does not maintain a centralised database on the ongoing and concluded ML investigations and therefore the statistics provided below is not comprehensive. However, the

[139] Police reports refer to either initiation of proceedings on the basis of open-source information; an ML case growing out of the investigation of a predicate offence –or the launching of a new ML investigation based on information received from a previous case.

following is information extracted from the national database for criminal proceedings maintained by the MoJ.

Table N°3.8: Number of ML investigation lead by different LEAs

Year	PBGB	ETCB	ISS	Prosecutor	No. information[140]	No. of terminated investigations	Total no of ML investigation
2015	25	16	1	1	7	0	50
2016	22	4			1	5	32
2017	34		1		2	9	46
2018	44			1	2	5	52
2019	17	1			1	10	29
2020	18	1				15	34
2021	12	0	0	0	0	9	21
Total	172	22	2	2	13	53	264

248. The number of ML investigations has decreased somewhat from the higher numbers in 2017 and 2018, and it is therefore questionable whether LEAs are maintaining the momentum in prioritising the investigation of ML.

249. Authorities indicated two reasons for this decrease. Firstly, that the focus of their work is on the complex ML cases involving large scale schemes. While the number of investigations is not high, the materiality of those is. Second is that ML investigations are time consuming while the sentences for predicate offences are usually higher than for ML offence (see 7.4). Examples have been provided where ML has not been pursued because the punishment for the predicate (e.g., drug trafficking) was more severe (up to life imprisonment) and that the investigation of ML could have, in the opinion of the authorities, hindered the success of the case and confiscation of assets.

250. It is also noted that there is an increase of the number of terminated investigation (20.08% out of all investigations for the period of 2015-2021 have been terminated). Authorities indicated the following reasons for the termination of ML investigations: (i) extradition of the offenders; (ii) absence of grounds for criminal proceedings; (iii) impossibility to identify the person who committed the criminal offence; (iv) and a decision by the prosecutor that the act only constitutes the predicate offence and not ML.

251. While provided reasons can be accepted as justifiable, as presented below there are thresholds set by jurisprudence that go over and above the legislative provisions, which may have hindered, and may continue to hinder, identification and investigation of ML offence. This is also recognised by some authorities and is highlighted to some extent in the 2020 NRA Action Plan. This includes:

- a threshold of EUR 15 000 as the amount of laundered property necessary to establish ML offence (Supreme Court Judgment no 3-1-1-85-11 from 14.12.2011 p. 46);

- a requirement of proving that the concealment of the illicit origin or the actual owner of the property *is condition sine qua non* (Supreme Court Judgment no 3-1-1-34-05 from June 27th, 2005, where the persons committing the predicate offence had bought cars using proceeds of crime and the Court concluded that not every use of criminal money is necessarily ML);

[140] Authorities indicated that for this column it was not possible to identify which authority led the investigation

- there must be a potential to harm the normal functioning of the economy (Supreme Court Judgment no. 3-1-1-68-10 from December 13th, 2010, and 3-1-1-94-14 from June 22nd 2015 where a thief had used around EUR 26 000 to build a sauna on his father's property. The Court stated the circumstances had no potential to harm the functioning of the economy and the offender did not have the intent of concealing the property and, therefore, no ML offence was committed);

- there is a requirement to prove a direct link between laundered proceeds and a specific predicate offence(s) which must be identified (albeit not proven); and

- not all tax offences are proceeds generating and therefore not predicate offences to ML, despite the fact that the Penal Code criminalises ML, following an "all-crimes approach". The Supreme Court does not consider it to be proceeds of crime when the perpetrator has retained a proportion of tax by virtue of a falsified tax return; it can only be proceeds of crime where the money has been defrauded through a tax refund.

252. Estonia does not have a system of binding judicial precedent and there have been examples of ML convictions contradicting those thresholds, including self-laundering cases. Therefore, this is squarely within the realm of an effectiveness issue rather than a technical one. Some of those judgments establishing high evidentiary threshold are more than 15 years old, but they are still quoted by the authorities (indeed they were mentioned in almost every meeting with LEAs, prosecutors, and the judiciary, often unprompted) and in the majority of instances used as an argument to explain the low number of ML investigations. It became evident from the meetings with the authorities and their written submissions, that the above presented jurisprudence is often taken into account when deciding whether or not to pursue a case but are not necessarily determinative.

253. Nevertheless, authorities presented ML cases where the value has been below EUR 15 000. This threshold could have inhibited prosecution of ML during at least part of the assessed period i.e., until 2017. It is said that legislative changes to the reporting threshold in 2017 ameliorated this issue, and therefore the threshold as argued by the judiciary (Supreme Court and lower courts) and prosecutors is no longer a binding rule.

254. In addition, there are case examples where the act was a pure self-laundering without any apparent potential to harm the functioning of the economy and still was considered as ML. However, some recent judgements by lower courts indicate that some of those principles are still applied.

Box N°3.10: County Court Judgement from January 9th 2020

Individual A was guilty of the acts described in the allegations of fraud, causing insolvency and committing tax evasion, whereby he received payment (around EUR 470 000) in his personal bank account and distributed a part of the money (around EUR 324 000) by making 10 bank transfers to company X. In addition, Individual A made 10 transfers from company X's bank account to company Y. The founder, shareholder and actual director of company Y was Individual A's life partner, Individual B. Individual A transferred the money from company X's account to company Y's bank account as agreed with Individual B. In addition, Individual B, who was also company X's bookkeeper, in cooperation with Individual A, deliberately left EUR 255 000 out of the balance sheet in company X's annual report. The Chamber based its view on the fact that neither the indictment nor the county court's decision indicated that the conduct described in Individual A's ML indictment was part of any wider, more permanent and universal scheme of conversion and/or concealment of property. According to the court, his alleged ML act did not have the complexity and scale that

would have given it an independent quality. Despite the transfers, a traceable connection remained between Individual A and the money received by him. Thus, the assets obtained by the crime, when making the bank transfers described in the accusation, and the recording of false information in the annual report of company X, as a concealment activity, did not qualify as ML.

255. The issue of tax crime as predicate for ML is potentially mitigated by the fact that the ETCB has an obligation to collect unpaid tax and will pursue this. Yet, the concerns remain that this case law is placing another gloss on the ML offence (for evasion or non-payment of tax) and could prevent possible ML cases where the offender has laundered money which he or she should otherwise have paid to the state and has avoided doing so by virtue of a criminal offence. The following is an example where ML has not been pursued in a tax infringement case because of the Supreme Court jurisprudence:

Box N°3.11: Investigation initiated by the ETCB– Tax infringement

In 2015 authorities launched criminal investigation for both tax infringement and ML offence. Nevertheless, the Prosecutor's Office decided that there were no grounds to prosecute for ML and sent the case to court in March 2021, prosecuting 6 natural persons for tax infringement for over EUR 4 million. The damages were not fraudulently received from the state budget but constituted unpaid tax, i.e., VAT and fuel excise. Therefore, the PO decided not to pursue ML charges.

256. The authorities indicated that they regularly conduct parallel financial investigations in order to establish proceeds of crime and enable, seizure and confiscation of the assets. In most cases, the ARO is the competent authority to conduct parallel financial investigation, but the authorities advised that other LEAs, when investigating predicate offences, also conduct parallel financial investigations. The authorities provided statistics on the number of financial investigations lead by ARO only (See IO 8, Table 3.15), which does not represent the total number of financial investigations conducted by Estonia. However, no information is available on the number of ML investigations triggered by financial investigations.

257. The analysis below indicates that LEAs do not effectively identify potential ML by using all available sources of information and intelligence, which potentially causes missed opportunities.

258. A recent investigation on complex ML schemes, involving a bank, shows that regardless of information available such as the EFSA reports (2014) and the whistle-blower information (2015) that was pointing that a significant amount of money was laundered for a number of years (2007-2015) in Estonian branch of bank D, the formal investigation was started only in 2017. Authorities asserted that those cases are given high priority, with resources applied accordingly.

Box N°3.12: Bank D

In November 2017 an investigation was launched, against Bank D 15 former employees, client managers for laundering USD 1 611 963 711 and EUR 6 074 878. During 2008–2015, suspected employees, while being aware of the criminal origin of money, deliberately failed to fulfil AML requirements and allowed foreign proceeds (at least 8 criminal activities taking place in different countries) to be laundered in Estonia. The laundered funds were transferred to 77 companies who had accounts in Bank D, and later in a layering phase transferred to 425 other companies' accounts. Furthermore, suspected employees advised clients on the methods for concealing BOs and by themselves were selling offshore companies to bank clients.

Between 2007 and 2014, the EFSA had conducted 15 supervisory activities, including six onsite inspections in the Estonian branch of Bank D. In 2015, based on an extensive inspection report, the EFSA issued a precept which forced

the branch to exit from non-resident banking. As a result of the EFSA's inquiries, the manager of the branch was removed by the parent company. In 2015 a whistle-blower reported to the EFSA that account books in the bank was not correct. At that time, the EFSA had already issued a precept and addressed the risk emerging from non-resident customers, without any further actions taken on the basis of the whistle-blower's insights. The EFIU, based on the analysis of the information coming from foreign requests, its own information and the EFSA's onsite inspection report, in 2017 filed a criminal report to both PBGB and the OPG.

During the course of criminal investigation, authorities, amid other investigative actions, identified and analysed at least 129 MLA requests previously submitted to Estonia regarding accounts of Bank D. In order to obtain evidence, 30 MLAs and EIOs were sent to 18 countries.

Within the extended confiscation regime, assets of both the suspects and third persons in total worth of EUR 9 855 549,77 have been seized in Estonia including ca EUR 2 000 000 in Latvia and EUR 100 000 in Liechtenstein.

Authorities have not initiated investigation of any legal person so far, even though employees of the branch of the Bank D have been involved, as well as a number of foreign companies. The JIT has been formed with the home country of the bank, which according to the authorities was planning to initiate criminal proceeding against the bank even though the Estonian branch had been closed. The investigation, at the time of on-site, was at the stage of final preparation for the court proceeding.

259. The authorities are rarely pursuing ML in parallel with serious domestic predicate offences, despite the principle of legality, and this could be impacted by the jurisprudence issues referred to above. This raises concerns since the sectoral risk assessment conducted by the EFSA estimated that in Estonia, domestic proceeds potentially laundered are in the amount of 120 million per year[141]. In addition, on the basis of statistics provided in the table below, while the number of investigations for domestic proceeds generating crime is not insignificant, the ratio of ML investigations to investigations into predicate offences is low.

Table N°3.9: No of investigations for predicate offences

	2015	2016	2017	2018	2019	2020	2021
Participation in an organized criminal group and racketeering	29	32	25	19	6	2	3
Terrorism, including terrorist financing	3	2	0	0	1	1	1
Trafficking in human beings and migrant smuggling	22	19	20	15	21	20	13
Sexual exploitation, including sexual exploitation of children	443	217	224	265	300	190	313
Illicit trafficking in narcotic drugs and psychotropic substances	1042	726	912	817	832	317	284
Illicit arms trafficking	238	126	143	138	131	138	127
Illicit trafficking in stolen and other goods	243	206	157	133	86	68	55
Corruption and bribery	323	47	53	57	38	43	22
Fraud	885	821	777	775	1155	1304	2202
Counterfeiting currency	10	4	1	1	6	1	6
Counterfeiting and piracy of products	12	11	16	14	6	11	5
Environmental crime	22	35	39	18	30	24	28
Murder, grievous bodily injury	148	128	120	136	114	127	101
Kidnapping, illegal restraint and hostage-taking	56	45	30	44	36	41	37
Robbery or theft	11691	7272	5629	5485	4788	4462	4629
Smuggling	36	12	12	6	8	6	7
Tax crimes	68	30	22	18	26	13	5
Extortion	123	71	70	71	72	62	58

[141] Sectoral money laundering and terrorism financing risk assessment, p. 18

Forgery	494	471	642	400	426	366	128

260. The co-operation and collaboration between the investigative authorities, the POs, and when necessary, the EFIU and FSA, appears strong.

261. JITs are often formed and in particular may be set up where there is a foreign predicate offence, complex ML or the matter involves a bank. There are examples of JITs formed with international counterparts for large scale suspected ML, including the "Bank D" case and the "Butterfly" case.

Box N°3.13: JIT Butterfly

In October 2020, criminal proceedings were initiated against four natural and one legal person (CSP) in a case which involves nearly EUR 45 million being transferred from a foreign state enterprise to a company in Estonia between 2013 and 2020. The EFIU received initial information from a foreign counterpart as part of an incoming request but was not allowed to domestically share it. However, the EFSA while performing its own duties, filed an STR later and the EFIU initiated a domestic case based on which investigation has been triggered.

The ML case relates to predicate offending of embezzlement around unjustifiably high-value public procurements. A dedicated team of national authorities including the ETCB has been set up. International co-operation has and is being used and a JIT was formed with authorities from the country where the state enterprise was formed. Investigative techniques such as surveillance, searches and seizure have been utilised, databases searched, and enquiries made to banks.

To safeguard the confiscation of assets, EUR 1 298 680 has been seized or subject to restrictions (e.g., for real estate, entry onto register preventing sale, mortgaging etc). It is considered by the authorities that Estonia was a transit country in this case – and that the majority of the funds did not remain in Estonia. The proceeding is ongoing.

3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

262. The NRA identifies the following crimes to represent the highest threat: computer fraud and fraud committed abroad, corruption and embezzlement committed in CIS countries, tax crimes committed in European countries, and, to a lesser extent, drug trafficking. Broadly speaking, authorities also indicated the misuse of e-residency programme, CSPs and VASPs for ML purposes (see IO 1). Estonia does not keep statistics on the underlying predicate offences for ML investigations. The examples of ML investigations and prosecutions show that computer fraud or fraud committed abroad are prevalent offences for ML. Authorities estimate that those account for 90% of ML cases. A common typology is that accounts are opened in the names of Estonian residents and companies, the proceeds of crime are transferred to them, monies sent to different bank accounts and then withdrawn or transferred abroad. According to the authorities, assets rarely remain in Estonia which is said to be a transit point for significant assets. There are altogether three CSPs and three VASPs currently under investigation, and in 2019 one natural and one legal person offering CSP services were convicted of ML. No examples of e-residents being investigated or prosecuted for ML were presented. The following case examples have been presented by the authorities to demonstrate ML investigations and prosecutions in relation to high-risk predicate offences.

Box N°3.14: Tirmaste and others

In 2017, seven persons were convicted for membership in a criminal organisation and ML and sentenced to 4 years' imprisonment. They were charged for laundering the proceeds of crime (tax offence) committed in neighbouring countries. The total amount of laundered proceeds was EUR 117 516,13. The members of the criminal organization founded companies in many countries (including Estonia). Those companies hired so-called shadow persons whose job was to conclude fictional contracts, make transactions between accounts providing false explanations, withdraw cash from ATMs, etc.

Transfers were made to bank accounts of companies under control of the criminal organisation, and money was withdrawn from bank accounts of the given companies. By means of different transactions and activities, the true nature of the funds and their criminal origin was concealed.

The investigation was triggered by intelligence gathered by the ETCB. The persons were convicted and 10 metal plates (platinum) with a value of EUR 266 478,20 and cash in amount of EUR 3 975 were confiscated. However, out of this EUR 1 175 was confiscated as proceeds of crime and the remainder as extended confiscation.

Box N°3.15: Case Hirvi

In 2019, two natural persons were convicted for fraud and ML, the investigation against them was launched in June 2018 for laundering EUR 634 896,65.

The predicate offences were fraud committed abroad by group of persons (so called Business Email Compromise ("BEC") or frauds of business letters). In order to conceal the origin of money that was received to the account as a result of the fraud and its actual beneficiary, economic transactions which were given legal appearance were performed. The role of a person A was to find a company which could be used for accepting funds originated from fraud committed in foreign countries. Person B agreed to participate in scheme by founding a company and using different bank accounts for the company where the fraudulently obtained funds were transferred to.

The EFIU restrained assets under precept in amount of EUR 634 896.65, which were further seized to secure claim for damage by victims.

The court convicted two natural persons in August 2019 for fraud and ML, sentencing each of them to aggregate 5 years of imprisonment and returned seized assets to victims under civil procedure.

263. In terms of national AML policies, the joint declaration of Laulasmaa between the Minister of the Interior and the Minister of Justice (re-confirmed in 2021) sets the anti-crime priorities of the government. This includes, *inter alia*, increasing the identification and confiscation of proceeds of crime and the proclaimed international ML in the financial sector and high-cost economic crimes as a common priority of the Prosecutor's office and the PBGB. These high-level goals are fairly generic and so it is not possible to conclude whether the ML results are in line with them. However, Estonia has demonstrated a risk-based approach through increasing its resources to pursue ML and high-risk predicate offences, and in particular, by creating specialised units. Some of the authorities did, however, express concern that their resources were not sufficient e.g., the PO.

264. The risks relating to high-proceeds-generating offences committed domestically, such as organised crime, smuggling of goods, human trafficking have not been sufficiently considered and assessed in the context of the ML risk (see IO.1). The number of ML convictions compared to the number of convictions for identified high risk criminal offences which can be predicate offences for ML are in context low. The total number of ML convictions over 5 years period was 78 against

170 persons, whereas the total numbers for potentially high proceeds generating offences in the same period were as follows: OCG involvement (324); drug trafficking (3 463); corruption and bribery (147); and fraud (1 482). This suggests that opportunities for pursuing ML are not being fully exploited as regards domestic criminality. Whilst it is accepted that ML will not be present in every offence, and that for many drug trafficking offences the proceeds may be low or drugs might be used for daily consumption, there should be a clearer assessment during the investigation of those crimes posing threat to ML. Nevertheless, some case examples have been presented where ML was investigated alongside organised crime and bribery.

Box N°3.16: Case Milli

In 2019, one natural person was convicted for accepting a bribe and ML. The Investigation launched in April 2015, with the PBGB investigating bribery in public procurement and later suspicion of ML.

The predicate offence took place in Estonia and the perpetrator was the head of the infrastructure department of public organisation. He received a bribe in order to manipulate the terms to allow the preferred companies to succeed with the procurement.

For requesting a bribe, fictitious invoices were issued. In order to conceal the origin of unlawful instruments, the defendant concealed it through transactions of his companies. The total amount of laundered property was EUR 105 333. The defendant was convicted for ML offence (two years and three months' imprisonment) and the following assets were confiscated: 9 gold coins with value of EUR 10 553, cash in the amount of EUR 92 048,69 on a bank account and a vehicle with value of EUR 23 447,50.

265. Misuse of legal persons (including CSPs and NPOs) for ML purposes was outlined in the NRA identifying that there are cases where companies are set up, money is transferred from a foreign country to Estonian bank accounts and further transferred to a foreign jurisdiction. Even though in some complex ML investigation one bank has been investigated (please see Bank S case below), generally legal persons are rarely prosecuted, and CSPs have also not been prosecuted to a great extent.

266. As regards criminal liability of legal persons, authorities indicated there is a legal requirement for the crime to be committed in the interest of the legal person and by senior executives who are the 'controlling mind' of the legal person or competent representatives. Reported offences have not been often committed in the interests of the legal person but rather the company has been (ab)used to move the money without it benefiting. Also, the legal persons are often turned to be shell companies with no assets and are liquidated immediately after the crime has been committed. However, while those arguments can in certain cases be reasonable, it raises concerns as that the ratio between the estimation of the legal persons being abused and the ones prosecuted is very low.

267. As regards the legal persons, Estonia has had ML convictions as follows:

Table N°3.10: Number of ML convictions for legal persons

Year	Legal person
2015	5
2016	2
2017	3
2018	1
2019	1
2020	1

2021	0

268. It is also worth mentioning that authorities in a recent large-scale case initiated criminal proceedings against a legal person (one bank), but the effectiveness is yet to be demonstrated since the process is still ongoing (see Box N°3.17: Bank S).

Box N°3.17: Bank S

In 2019, the PO, based on the EFSA report, initiated an ML investigation against nine natural persons (employees and CEO of the bank) and one legal person - Bank S, because of suspicions of laundering proceeds of crime (in total EUR 80 million) emanating from foreign countries in the period of 2014-2016. Suspected persons made ostensibly legal transfers with the aim of concealing the real origin and ownership of funds.

The volume of the criminal case is characterised by the number of companies investigated and involved in ML. The group of companies through which ML was carried out included 42 legal persons. The object of the investigation is the movement of funds within a financial institution between the accounts of different companies, and the concealment activities concerning the transfers. Authorities gathered evidence from financial institutions (76 inquiries) and through co-operation between the LEAs, FIU and EFSA which appeared to be productive.

No assets have been seized in the criminal case, but 15 MLA and EIO requests have been sent to identify the assets suspected to be located in foreign countries.

269. It can be concluded that so far, the achieved results are to some extent in line with the risk profile of the country i.e., foreign predicate offending, but this is caveated by the issues identified under IO.1 on the country's understanding of its risk. There are issues with ML being pursued as regards domestic high-risk offences and only to a low extent against legal persons and CSPs, but it is also acknowledged that Estonia is focusing more of its efforts on large scale complex cases.

3.3.3. Types of ML cases pursued

270. Prosecutors and LEAs have demonstrated that they can pursue all types of ML offences (third party, self-laundering, stand-alone) and they have indeed achieved results for each, including self-laundering, notwithstanding the judicial interpretation issues. In total, in the period 2015-2020, ML convictions were achieved in 78 cases against 170 persons. There are no statistics available on the different types of ML prosecution, but the following table shows the numbers of different types of ML conviction (by case).

Table N°3.11: Different types of ML convictions

Year	Total cases	Self-laundering	Third party ML	Foreign predicate offences
2015	17	5	12	14
2016	15	1	14	11
2017	12	3	9	7
2018	11	4	7	7
2019	11	3	8	9
2020	12	3	9	6
2021	11	0	11	11
Total	**89**	**19**	**70**	**65**

271. Despite the fact that some case examples and statistics of self-laundering ML have been presented, the interpretation of ML offence by Supreme Court jurisprudence raises concerns as to what extent self-laundering is being investigated and prosecuted. This has been alluded to under Core Issue 7.1 and is the requirement for there to be an act of concealment and harm to the

orderly functioning of the financial and economic system. As one authority said, this makes incriminating self-laundering practically impossible. Evidently, the results demonstrate that it does not exclude all possible types of self-laundering cases and they have achieved self-laundering convictions. It is, however, clear that this restrictive interpretation has harmed effectiveness for such type of ML cases. It is accepted that there is value in prioritising more complex ML such as third party and foreign predicate offences and Estonia is commended for doing so; however, this does not justify setting a standard which could exclude self-laundering depending on the judge dealing with the case.

272. Authorities indicated that a conviction for predicate offence(s) is not a prerequisite to convict for ML, and autonomous ML offence can be pursued without obstacles. However, the predicate crime must be identified and a direct link between predicate crime and laundered property should be established. Although this does not fall foul of R.3, this may nonetheless inhibit effectiveness for the prosecutors to be required to establish the precise predicate offence and such a link even when there are otherwise irresistible inferences that the money arises from criminality, and notwithstanding that the legislation allows ML to be established "*also where the details of a criminal activity which generated the property to be laundered have not been identified*."[142]

273. Estonia provided examples which demonstrated that it does, on occasion, appeal against ML acquittals including one example where the prosecutor appealed (unsuccessfully) the Court's acquittal due to it considering that the activities did not have the potential to harm the functioning of the economy.

274. The authorities presented a successful case of autonomous ML conviction where the foreign predicate crime was only identified, the perpetrator was not, and in Estonia an ML conviction was achieved.

Box N°3.18: Autonomous ML

In 2020, one natural person was convicted for ML. The Predicate offence was fraud. It was committed in a foreign country (and the perpetrator was not identified). The case originated from the EFIU dissemination. The person was convicted in Estonia for concealing unlawful origin, ownership and location of money on amount of EUR 559 876,77. It was sufficient for the statement of claim lodged in foreign country to confirm the commission of the predicate offence in that country.

The foreign company received an email where they were asked to pay invoices to a new bank account. The funds were transferred to the new account and later on it became evident that these accounts belong to fraudsters and not to the actual companies who presented invoices.

In order to conceal the unlawful origin, ownership and location of EUR 559 876,77 emanate from fraud, transfers were made in different accounts, also money was withdrawn in cash, constituting ML activities. In order to conceal the unlawful origin of money and transfers made, documents reflecting procurement and movement of goods were prepared. Transfers were made to a bank account that belonged to an Estonian company. The defendant was one of the persons who made the transactions to hide the illicit origin of these funds. The defendant was convicted in general procedure (case went up to Supreme Court) and was sentenced to 2 years 6 months of imprisonment for ML. 2 more

[142] Section 4(5) MLTFPA

natural persons and 1 legal person were convicted for ML under the settlement procedure. In this case, a total of EUR 55 104, 33 was confiscated.

275. Around 75% of ML convictions are for third-party laundering. In many instances the typologies are not complex. However, there are some good examples of convictions for third-party ML presented.

Box N°3.19: Third-Party ML

An investigation was launched in 2011 and 5 physical and 5 legal persons were convicted in June 2015 for ML.

The proceeds were suspected of being generated through cyber fraud in Estonia and in the USA by 2 natural persons. Defrauded proceeds of USD 21 936 547 and EUR 234 700 were transferred through different accounts in several countries before ending up in the accounts of 5 legal persons in Estonia. The ML was prosecuted autonomously and under the aggravated offence. Two persons were convicted of self-laundering and the others - for third party ML.

The main leader was punished for ML offence and formation of a criminal organisation with real imprisonment for 6 years, which is rare in Estonian court practice (usually imprisonment is conditional and unenforced). Monies and different property were confiscated from the perpetrators with a value of EUR 19 274 970. Legal persons were sanctioned with fines ranging from EUR 20 000 to EUR 100 000.

The USA shared assets totalling nearly EUR 800 000 with Estonia for its co-operation with the US authorities leading to forfeiture in that jurisdiction.

276. To Estonia's credit, the majority of ML prosecutions and convictions are for ML with a foreign predicate offence (approximately 70%). Furthermore, the majority of offenders are third party launderers, and the authorities reported that 40% of cases are prosecutions and convictions achieved for autonomous ML.

277. There are delays (sometimes for years) in some court proceedings which could affect the cases reaching judgement albeit it is said by the authorities that this was not typical in ML cases and provided some statistics on cases which have reached final verdict in reasonably prompt fashion, with the settlement procedure being used regularly, but those which went to trial (general procedure) also completing in a reasonably expeditious manner.

278. Whilst some delays in trial procedures have been observed these issues tend to be more prevalent in larger and more complex cases. Defence counsel uses various tactics to cause delays, in order to postpone trials and prolong procedure. Whilst fundamental rights continue to be protected, the authorities have used methods to mitigate issues with delay such as using video technology, which have allowed hearings to proceed even if parties are unable to attend physically. Such practice is welcomed and on a positive note Estonia set up a group within the MoJ, including a judge currently on secondment, to analyse the backlogs and propose ways to resolve issues of delays in trials. Statutory time limits were not said to have caused any issues, including for appeals, as the limitation period is interrupted by the prosecution of the accused.

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

279. The sanctions available to the authorities can be considered effective and proportionate, albeit not fully dissuasive (see Criterion 3.9). The sanctions applied in practice in Estonia for ML offence are not effective or dissuasive, particularly when compared with the sanctions for other serious offences, even though they might be considered proportionate.

280. The vast majority of custodial sanctions imposed for ML offences are conditional meaning that perpetrators are imposed with suspended imprisonment which is rarely actually enforced. However, even the average conditional sanctions are at the lower end of the available scale.

Table N°3.12: Average prison sentences imposed within conditional sanction

Year	Average prison sentence (years)
2015	3 ½
2016	1 ¾
2017	2 ¾
2018	2 ½
2019	2 ¾
2020	2 ½
2021	3

281. Authorities indicated that there was a general sentencing policy in Estonia to avoid imprisoning offenders, especially for first-time offenders in order to try to rehabilitate them. Whilst not imposing imprisonment sanctions in less serious cases might be sometimes justifiable, it causes a danger that such sentencing policy will not act as a deterrent to others. This is particularly so for cases presented by the authorities in which a sentence was conditional[143] despite the offence appearing to be serious because it involved (i) the aggravated offence, (ii) large sums of suspected laundered cash, or (iii) abuse of the Estonian financial system to launder foreign proceeds of crime. Thus, such sanctioning policy suggests that ML is still not treated as serious criminal offences. It was acknowledged that economic crimes are not always treated as serious by the judiciary compared to serious predicate crimes such as drug trafficking which are more likely to results in actual imprisonment. Having a criminal record and a conditional imprisonment sentence may entail inconvenience, restrictions and shame (as asserted by the authorities) but this does not reflect the seriousness of the ML offence and therefore the sentences applied (overall) cannot be considered to be effective and dissuasive.

282. In fairness, the authorities provided some case examples where the imprisonment sentence (and other sentences) imposed in those cases can be said to be dissuasive. In a number of cases, the imprisonment sentence was up to 7 years albeit this was usually the aggregate sentence when combined with a predicate offence and such cases were the exception rather than the norm. No examples of a sentence ever being appealed by the prosecutor were provided.

283. Estonia has a substantial practice of using plea bargaining agreements to settle ML prosecutions. It has enabled the jurisdiction to achieve some good results and release resources to deal with other cases, it has also likely contributed to the low levels of sanctions.

284. The fines imposed on legal persons for ML are usually a four figure or five figure sums; in the statistics provided the average amount fines ranged mostly from EUR 4 000 to EUR 5 000. In 2015 the overall average amount of fine was higher as it was affected by one case (Box N°3.19 Third-party ML). In that case fine in the amount of EUR 100 000 was imposed on one of the legal persons. The level of other fines applied in 2015 were in the same range as above. Hence, this was rather an exception than a norm.

[143] Some examples: Aasa and Metsik, Martin and Others, Leppik, Lashenko, Volonko and others, Semiskar

285. The authorities noted that supplementary punishment can be applied, such as restricting natural persons from economic activities for a set period. Nevertheless, no examples were provided of regulatory measures applied following an ML conviction. In Estonian legislation there is no sanction for legal persons such as removal from the register.

3.3.5. Use of alternative measures

286. Estonia can apply extended confiscation, and in convictions for predicate offence it has done so together with severe imprisonment sentences. Authorities presented several case examples where conviction for a predicate crime(s) was followed by an order of extended confiscation (in one case imprisonment sanction was 7 years and extended confiscation was applied in the amount of EUR 1.2 million).

287. While extended confiscation can be a useful tool when due to the "justifiable reasons" ML conviction was not possible to secure, in the cases presented, the authorities did not pursue ML offence at all. Furthermore, the reasons for applying extended confiscation cannot be taken as justifiable for not pursuing ML since the reasons given were that the ML offence carries a lower sanction than predicate offence, or ML is not possible due to the restrictive interpretation of the Supreme Court jurisprudence, and lenient sentencing practice for ML. Such cases cannot, therefore, be given any weight when the reasons for not pursuing ML are those very same deficiencies identified elsewhere under IO7.

Overall conclusions on IO.7

288. Estonia has designated authorities to investigate and prosecute ML offence and appears to be reasonably well resourced but requires better resources in some areas. So far, the achieved results are to some extent in line with the risk profile of the country and the jurisdiction is to be recognised for its success in prosecuting many third-party ML cases and usually with an underlying foreign predicate offence. Nevertheless, authorities are not fully harvesting all potential investigations from available sources (such as MLA) and domestic criminality is not being fully exploited for potential ML. Estonia has applied resources and focus on larger complex cases. The number of legal persons investigated and prosecuted for ML is low.

289. Estonia pursues different types of ML, with a particular concentration on third party and/or autonomous ML and usually based on foreign predicate offending. There are issues with the narrow interpretation by the judiciary of ML offence. There may be mitigation as described above but such interpretation could hinder the jurisdiction's effectiveness in investigating, prosecuting, and convicting ML, and this must be addressed urgently. The sanctions for ML are not effective and dissuasive since they are low for natural persons and very low for legal persons, with imprisonment of natural persons usually suspended. Extended confiscation is used in cases where ML is not pursued but the reasons provided are not necessarily justifiable.

290. **Estonia is rated as having a Moderate level of effectiveness for IO7.**

3.4. Immediate Outcome 8 (Confiscation)

3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

291. Estonia pursues confiscation as a policy objective, but as discussed further below, the results suggest that, in practice, the policy is achieved to some extent. The Estonian Penal Code provides for the possibility to secure and finally confiscate proceeds of crime, instrumentalities, and property of equivalent value (substituted confiscation), and third-party confiscation. Confiscation proceedings may occur in parallel with the substantive criminal investigation or separately. All investigative powers can be utilised as part of any confiscation proceedings.

292. In order to make the crime unprofitable the Estonian legislation goes beyond the requirements of the FATF standards and allows application of extended confiscation of a part or all of the criminal offender's assets in certain circumstances. Precondition for such confiscation is court verdict convicting offender for a term of at least one year of imprisonment. In the extended confiscation proceeding assets may be confiscated if the nature of the criminal offence and the difference between the legal income and financial situation of the offender gives reason to presume that assets are acquired through criminal offence(s) (unless the person can certify they were not acquired by criminal offence). These provisions can apply in certain circumstances to mixed assets and to assets belonging to a third person.[144]

293. Whilst extended confiscation, confiscation of instrumentalities, and confiscation of equivalent value is discretionary, none of the authorities considered this to be an issue, nor were any problems raised with how the legislation operates in practice. The confiscation of property laundered and proceeds of crime is mandatory.

294. The deprivation of the proceeds of crime is endorsed in the overarching policies:

a) **Laulasmaa Declaration** (originally 2005 but re confirmed in April 2021) handed down by the Ministers of Justice and of the Interior sets, targeted activities to increase identification, seizure and confiscation of assets, as the priorities of the Government.

b) **Internal Security Development Plan 2020-2030** stipulates (i) the further need to develop pre-requisites for increasing the identification and securing proceeds of crime, (ii) training and raising awareness, specialist training for judges and officers, and (iii) setting up a national database to collect, store and analyse information on assets seized and confiscated.

c) **The 2020 NRA Action Plan** sets an obligation to strengthen legal aspects that hinder the efficiency and effectiveness of seizure and confiscation. The planned activity in respect of this is to proceed to develop administrative and civil forfeiture and non-conviction-based confiscation.

295. In addition to the governmental level, there are other strategic and operational documents setting up confiscation as priority such as the 2019 PBGB's Strategy "Guide to Identifying, Valuation and Accounting for Property Acquired by Offence and Extended Confiscation of Property" and Directives issued by the same organisation, emphasising the priorities for seizing and confiscating criminal assets. The ETCB, being an LEA with investigative competencies, follows

[144] Section 83[2] Penal Code

these strategies and the risk assessments, priorities, and guidance of the PBGB, to the extent they are applicable in investigations of tax and customs related crimes.

296. The creation of the Asset Recovery Bureau (ARB) in 2011, within the NCP, demonstrates the authorities' commitment of resources to tackle financial crime and deprive criminals of their ill-gotten gains, as a policy objective. The ARB has dedicated officers who can assist, when called upon, with investigations to help identify proceeds of crime. The ARB is based within the NCP. The police prefectures also employ criminal asset investigators.

297. The ETCB has, as its strategic target, to collect all state taxes. Financial investigations are said to always be a part of the tax and customs related criminal investigations the ETCB conducts. It has its own investigators who are specialists in seizure and confiscation of assets. There are three officers in the national headquarters and one in each of the three regional investigative units, thus further enhancing the dedicated resource to pursue confiscation as a policy objective at strategic level. The ETCB has annual training for its officers with the assistance of the PBGB and ARB.

298. There is no doubt that the authorities consider seizure and confiscation as an important policy objective, and as a priority. This is seen as such at a high level and at the strategic and operational level. However, achieved results follow set objectives only to some extent.

3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

299. There is a lack of comprehensive data on seized and confiscated instrumentalities and property. This has been acknowledged in the 2020 NRA Action Plan as one of the obstacles to conducting an assessment. Therefore, the assessment team based its conclusions on the data and case examples available to it.

300. In Estonia, compensation of the victims of the crime is given priority. Authorities indicated that whenever in a criminal case there is a claim by a victim(s) the court will decide first on this request and further proceed with a confiscation order. The estimation is that between 2016 and 2020, the total value of assets seized for civil claims was about 15% of the amount of assets confiscated in criminal proceedings. Whilst not criticising this approach, without comprehensive data it was not possible to fully assess the extent of the achieved effectiveness.

301. Even though confiscation of instrumentalities is envisaged in the legislation, as well as the possibility to order preventive measures, the authorities did not demonstrate effectiveness in this regard through statistics. The authorities stated that the objects used to commit crime are confiscated on a regular basis and some case examples have been presented where instrumentalities such as drugs and weapons have been confiscated. When deciding on confiscation of instrumentalities, on case-by-case basis, the proportionality is considered, as well as the efficacy of confiscating instruments. Some examples were provided where the instruments were not confiscated even though it appeared to have been appropriate to consider doing so.

302. Confiscation of proceeds from ML and predicate offences in Estonia has been achieved to some extent. The authorities demonstrated overall figures and no breakdown was available between proceeds confiscated from domestic and foreign predicates. In addition, there is no breakdown between laundered property, property of equivalent value and the value of property confiscated in the framework of extended confiscation.

Table N°3.13: Seized and confiscated property (in EUR)

	2015	2016	2017	2018	2019	2020	2021	Total
Seized property (ML)	230 467	337 396	1 771 070	574 174	1 142 025	2 742 943	0	**6 798 075**
Seized property (predicate offences)	3 315 934	9 666 213	5 426 223	9 850 442	9 552 805	5 525 270	5 146 146	**50 784 291**
Total Seized Property	3 546 401	10 003 609	7 197 293	10 424 616	10 694 830	8 268 213	5 146 146	**56 431 737**
Confiscated property (ML)	18 915 598	573 735	631 366	534 868	2 074 888	163 947	134 247	**23 028 649**
Confiscated property (predicate offences)	4 848 030	3 502 738	6 252 648	2 447 973	6 155 456	2 687 081	1 637 643	**27 531 569**
Total Confiscated Property	23 763 628	4 076 473	6 884 014	2 982 841	8 230 344	2 851 028	1 771 890	**50 560 218**
Total Recovered Property	n/a	n/a	n/a	n/a	3 901 106	2 115 962	1 100 815	**7 117 883**

303. The overall figure of assets subject to confiscation orders for ML and predicate offenses in the assessed period is around EUR 50 million, which is not an unreasonable overall figure. Nearly half of this was confiscated in 2015 (mainly due to the Third-Party ML case, see IO.7) and the average annual figure between 2016 and 2020 was around EUR 5 million. The jurisdiction does not have an estimation of the overall proceeds of crime but considering sectoral risk assessment conducted by the EFSA which estimated that in Estonia, domestic proceeds potentially laundered are in the amount of EUR 120 million per year, it is questionable whether the results are proportionate to the potential overall value of proceeds of crime, whilst nonetheless recognising that Estonia is often used as a transit country.

304. Estonia provided several examples of cases where large confiscations were ordered. These were usually extended confiscations, which is a useful tool, but the assessment team was not convinced that the jurisdiction was adequately tracing and seizing the proceeds of crime where possible which could lead them to initiate further ML investigations and asset recovery.

305. There have been some examples provided where proceeds of crime have been seized and confiscated.

Box N°3.20: Large-scale confiscation

The PBGB initiated a criminal investigation based on open-source intelligence combined with information from international (non-EU MS) partners. According to the suspicions, the criminal offender was active in different cybercrime and fraud related fora and advertising professional ML service for a fee 10-55% from each transaction. The exact total amount of laundered money is not known, but as his fee was from 10 to 55%, a very conservative estimation is that at least EUR 3 000 000 were laundered. His services included using bank accounts and e-wallets opened for physical and legal persons in multiple different jurisdictions. The ARB led a financial investigation alongside the substantive criminal investigation to identify and seize proceeds of crime. Assistance was sought from multiple jurisdictions where assets, such as, real estate, motor vehicle, crypto currencies were seized. The total value of seized and later confiscated assets was approximately EUR 1 210 036.

306. It is important to stress that there have been examples of seizing and confiscating VAs which is a positive step. Authorities advised that in one ML case they identified, seized, and confiscated VAs held in the convicted person's user account held with a VASP. Nevertheless, authorities did not provide details on the methods used to identify VAs.

307. Criminals laundering money in Estonia are said to use seemingly unconnected individuals and legal entities as money mules, using infrequent and small sums. Notwithstanding the difficulties this creates with detecting financial crime, the authorities' methods of following the money trail in financial investigations has led to the detection of connections and the confiscation of assets from third parties.

Table N°3.14: Criminal assets seized from third parties

Year	No of criminal cases	Amount of criminal proceeds seized from third parties (in EUR)	No of persons involved
2015	24	835 123,55	42
2016	22	1 514 729,40	41
2017	24	1 513 226,70	39
2018	22	2 076 305,36	53
2019	16	1 787 015, 59	29
2020	21	3 418 481,56	27
2021	14	1 133 761,08	20
TOTAL	143	12 278 634,24	251

308. In order to secure confiscation (included extended), the authorities asserted that they trace proceeds and order preventive measures to secure those proceeds in both ML and predicate offences.

309. Financial investigations aimed at tracing and securing proceeds of crime, as well as assets subject to extended confiscation are said to be regularly launched, as part of the investigative process, to determine assets involved. Nevertheless, authorities do not keep statistics on the number of financial investigations, except when conducted by the ARB.

310. The majority of financial investigations are carried out by the NCP, and in complex and high-profile cases by the ARB. The record of seizures with ARB involvement (as the below table shows) is commendable comparing to the overall seized assets. The police prefectures and the ETCB also conduct financial investigations, using the assistance of the ARB where necessary. Financial investigation begins with the identification and mapping of assets, including the possible origin of the assets, and of persons enriched by criminal activities and associated persons. Whilst there is no written guidance on when a parallel financial investigation could or should be launched, Estonian authorities follow the policy that crime should be unprofitable. The PBGB (including the ARB) and the ETCB, when conducting parallel financial investigations, have direct access to wide range of information from variety of databases (see IO.6).

311. The ARB has been involved in the most complex and high-profile cases, particularly involving financial institutions. The record of seizures with ARB involvement is shown in the below table and demonstrates the efficacy of ARB involvement.

Table N°3.15: ARB investigations and seizure

Year	No. of investigations started in the ARB	Seized assets further to the ARB investigations (in EUR)
2015	24	2 958 026
2016	42	8 948 931
2017	39	6 724 248
2018	11	12 746 708
2019	17	2 169 974
2020	31	1 880 666
2021	23	2 023 054

312. As mentioned above, there are questions on whether proceeds of crime are being adequately traced. However, extended confiscation is exercised as a useful tool to shift the burden of proof onto a person convicted of an offence and confiscate all of his or her unexplained wealth. Substituted confiscation is also used effectively to ensure persons are nonetheless deprived of assets regardless of whether the actual proceeds are still available.

313. The EFIU has a powerful mechanism to issue suspension orders i.e., precepts[145]. It can issue the precept to suspend a transaction or impose restrictions on the disposal of property. The authorities met confirmed that these measures were used regularly to safeguard assets. Other measures are also utilised, such as entering restrictions on the land register to prevent the sale, dissipation or lodging of a charge against immovable property.

314. As would be expected, the figures are lower for ML confiscation than for seizure. Money estimated be to be laundered was significantly more. The authorities explained that Estonia was often a transit country and very little of the monies remained in Estonia or part of the seized money was used as compensation for the victims of predicate crime. There are also several other reasons for such outcome, for example the misinterpretation by the authorities of ML offence may influence the overall achieved results in ML convictions and therefore in confiscation. The high-level evidentiary threshold appeared to cause in one example the release of a large amount of funds suspended using EFIU suspension (several million Euros). Further, issues identified under IO.7 as regards delays during the court proceedings can also be a factor in delaying the confiscation of assets.

315. Property owned by legal persons has been seized and confiscated and the authorities gave examples of the shares of companies being seized. Otherwise, legal persons are not regularly seized themselves. There is no type of asset which cannot be confiscated but the majority of items have been tangible movables (including cash), real estate or monies held in bank accounts.

316. Estonia estimates that they are largely used as a transit country to launder proceeds. Nevertheless, the authorities did not adequately demonstrate that they effectively seek, and confiscate proceeds moved abroad (see IO.2). The general view of the authorities was that this is not their priority since it is moved from a foreign country through Estonia to another foreign country. Some examples of efforts to trace and recover property from abroad were, however, provided.

[145] S. 57(1) MLTFPA

Box N°3.21: Pursuing assets abroad

In 2021, the Southern Prosecutor´s Office sent an EIO request to a neighbouring country to trace assets obtained by offender who was suspected of leading the organised crime group which had stolen expensive cars in Estonia. As a result of the EIO, the assets in country L were identified and seized in a value of EUR 22 976. Foreign authorities transferred EUR 11 750 to Estonia to compensate the victims.

317. As demonstrated by Table 3.13, the authorities were able to provide some statistics on the property actually recovered. Considering the data provided, it can be concluded that the majority of confiscated assets for given years were recovered, but still, due to the limited information it is difficult to substantiate the overall effectiveness of the regime.

318. As regards asset management, this is an important mechanism given the issues with some court delays and the risks of property losing its value whilst seized and awaiting the confiscation order. Indeed, the authorities identified depreciating assets as a potential vulnerability in the NRA and the 2015 Action Plan targeted the issue of long proceedings and high storage costs and the efficiency of the asset realisation system. It was said that this was being addressed through additional resources and trainings of officials. There is no specific asset management office, which the authorities may wish to consider the utility of. The asset management work is mostly done by the PBGB and ETCB. For the PBGB, the Logistics Bureau deals with the handling (storage, return, destruction, and transfer) of physical evidence, findings, seized assets and is also involved in the sale of confiscated assets.

319. The Government regulation[146] requires seized property to be kept in a manner that ensures the preservation of property, or it is transferred to specialised storage premises to ensure the preservation of its value. The state has several arrangements in place for particular assets with private contractors, such as a storage place for high value vehicles and the movement and preservation of particular assets such as precious art. There have been examples of depreciating assets such as vehicles and perishable items such as fish, being disposed of to preserve the value. The sale of a seized asset can only be granted by court order (either with or without the agreement of the owner - the former obviously being more straightforward to get the court approval). There does not seem to have been any issues with this in practice and the Supreme Court has provided guidance in their decisions on the competing interests between the individual rights and the need to thoroughly substantiate an interference with the individual's rights to be sanctioned to dispose of the asset.

320. Physical property is stored at the Logistics Bureau by the person conducting the proceedings. The property is stored and logged using the system which was introduced in 2020 to maintain records of physical evidence, confiscated and seized assets and findings.

321. The authorities appear to manage different types of seized assets well. It remains to be seen, once more complex assets such as legal persons and VAs were to be become subject to seizure more often if the authorities would have adequate capacities and measures in place for these eventualities. Nevertheless, there was a case of managing VAs subject to seizure when the suspect was given the choice whether to keep the VA or convert it to standard currency, but no

[146] Government Regulation for Procedures for Transfer of Confiscated Assets Return of Money Received from the Transfer of Property to the Legal Holder from the State Budget, Registration and Destruction of Physical Evidence, Storage, Valuation and Transfer of Seized Property and valuation, transfer, and destruction of perishable evidence.

information was provided on the outcome of this procedure. Authorities advised that the PBGB has Guidelines on Asset Management allowing outsourcing when managing seized assets, if necessary. However, this guideline was not made available to the AT, and practical application is yet to be tested.

322. Confiscated assets go into the general State budget and are not specifically set aside (i.e., ring-fenced) to be used only for anti-crime purposes. This is not an issue *per se* nor a requirement of the standards, but it may be worth considering such a mechanism especially given the political commitments to continue increasing resources for fighting financial crime.

323. As regards asset sharing, Estonia was unable to provide any statistics of asset sharing with other jurisdictions. The authorities did, however, present one case example of a foreign jurisdiction sharing assets with Estonia (see IO.7 box: Third party ML). There have been no confiscations relating to TF (there was only one TF conviction and apparently no proceeds to confiscate).

3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI

324. Estonia has a land border with fellow EU Member State Latvia and one with Russia. Tallinn has an international airport with connections to destinations all around continental Europe, as well as Turkey. Other regional and commercial airports have limited destinations. There are several seaports in Estonia as well, with those in Tallinn, being the busiest.

325. Estonia operates a cash and BNI declaration system at its port entry points and borders but only for those entering from and leaving to outside the EU. Its system is based on EU Regulation 2018/1672. The lack of controls with EU jurisdictions is a technical deficiency[147] and may hinder the effectiveness of detecting cross border cash movements which could be related to predicate criminality and/or ML/TF especially considering risk and context of Estonia. The authorities use mobile units to carry out searches on passengers and visitors for suspicious goods regardless of origin and destination. A mobile unit carries out checks on roads near borders and at the ports. Checks are carried out on mail cargo and the authorities use measures such as x-ray, searches and sniffer dogs on the trucks, trains, passenger luggage and mail and cargo detect undeclared cash and other items (tobacco for example is a regular commodity for smuggling). The system does appear to be, nonetheless, comprehensive and efficient for all movement, regardless of origin and destination, and examples were given of cases involving EU passengers detected by the ETCB.

326. The authorities stated that there is prominent signage at the ports and borders advising persons of the need to make a declaration where necessary, by way of electronic televisions. At Tallinn airport, and in the eastern land border points, information about the obligation to declare cash is electronically available in several screens in three languages, Estonian, English, and Russian. Leaflets about prohibitions and restrictions for travellers are available in every border point (consisting of information about the obligation to declare cash), as well as on the ETCB webpage.

[147] See Recommendation 32

327. The ETCB contacts the EFIU immediately if there is any ML/TF suspicion, However, only limited statistics were available showing that in 2020, under the misdemeanour procedure, the ETCB notified the EFIU four times and in 2021, five. In addition, there is no information what the outcomes of the cases were. As noted in the technical review[148], the ETCB has the right to temporarily detain cash for up to three business days, and so may do when there is ML/TF or predicate suspicion.

328. The ETCB also has strong co-operation with the PBGB, particularly at border crossings where joint patrols are conducted. The ETCB has access to a PBGB database, which is used at the border crossing points for selecting passengers to physical control and personal data is inserted to the system. Data about persons who submitted false declaration or have failed to declare cash are entered into the system. This helps the ETCB to detect suspicious movements and carry out controls at the border and to be alert to previous offenders.

329. When a breach is detected, the ETCB can initiate misdemeanour or criminal procedure or, if there is suspicion of ML, TF or predicate offence(s), then a criminal investigation can be launched. In the misdemeanour procedure, authorities impose fines and in criminal procedure fines, imprisonment and confiscation can be ordered.

330. Authorities provided statistics on the number of declared incoming and outgoing cash as well as the number of the non-declaration (see table below). Some ML suspicions and only one TF have arisen out of non-declared or falsely declared cash, which raises concerns taking into consideration the risk and context of Estonia as a transit country.

Table N°3.16: Number of cross border declarations and non-declarations

Year	Incoming currency (in EUR)	Outgoing currency (in EUR)	ML suspicion	TF suspicion	No. of non-declaration
2015	31 825 914	52 884 357	4	0	11
2016	33 460 417	82 780 974	3	1	5
2017	24 699 342	101 513 613	4	0	11
2018	21 799 194	39 961 088	1	0	4
2019	26 442 324	25 321 780	8	0	19
2020	4 639 217	7 465 590	2	0	10
2021[149]	23 978 709	48 571 784	8	0	13

331. The following statistics were available based on the criminal procedure conducted for the criminal offence of non-declaration of cash exceeding EUR 40 000. In many cases the criminal proceedings were terminated (with the offender required to pay an amount to the state in lieu) and once fines ordered they were rather minor.

Table N°3.17: Property seized and confiscated in the criminal proceedings for non-declaration of cash

Year	Property Seized (EUR)	Property confiscated (EUR)
2015	70 500 EUR 35 070 000 RUB[150]	0
2016	47 880 EUR	0

[148] Recommendation 32.8
[149] The increase in 2021 is because the UK became a third country.
[150] 1 RBL=0,01 EUR

2017	159 460 EUR 654 050 RUB 220 PLN[151] 2 560 SEK[152]	0
2018	102 530 EUR	0
2019	399 995 EUR 71 855 USD 10 GBP 81 950 RUB 20 BYR[153]	176 800 EUR 81 950 RUB
2020	2 100 EUR 80 800 USD	0
2021	204 650 EUR	0

Box N°3.22: Non declaration of cash

In 2016, the ETCB's mobile unit detained a passenger car coming into Estonia from country L with EUR 323 000 of cash found in its boot during inspections, and the suspects had no documents to prove the origins of the money. The ETCB filed a report with the EFIU and sent the case for further investigation to the PBGB. The suspects had submitted contracts between foreign companies and previous loan agreements between Estonian companies to attempt to prove the legitimate origin of the cash. However, analysis by the EFIU, established that the individuals had committed large-scale leasing fraud through the Estonian companies. The EFIU issued a precept stopping the use of the cash for 30 days and filed a report with the OPG.

The two natural perpetrators were convicted of embezzlement and fraud and imprisoned for between 1 year and 2.5 years, and the cash was used for compensation for the victims.

332. As regards cash confiscated under the misdemeanour framework (used where the undeclared or falsely declared amounts are below EUR 40 000) figures were not provided, except for 2020. Seeing as this framework is used for the majority of the time, these statistical deficiencies impede the ability to assess the effectiveness of the regime. Figures were provided on the misdemeanour fines issued for undeclared and falsely declared cash between 2020-2021; nine fines were issued, the minimum EUR 140 and the maximum EUR 600. These were said to be for situations where there was a mistake by the passenger and where they have been able to prove the legitimate provenance of the cash. Recently, a lot of the focus has been on persons attempting to take Euros to a foreign country, which at the time of the on-site had occurred 13 times since this was prohibited as a result of the EU sanctioning regime, with the figures ranging from four to five figure sums. However, there is no information about sanctions applied in those cases.

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

333. The objective to establish an overview of criminal proceeds and the capacity to identify these was in the 2020 NRA Action Plan. Nonetheless, since most confiscations are based on extended and substituted confiscation, the authorities did not present specific measures undertaken to achieve this goal.

[151] 1 PLN=0,21EUR
[152] 1 SEK=0,09EUR
[153] 1BYR=0,001EUR

334. According to the authorities, the seizures and confiscations primarily occur in "so called high priority predicate offences." The available statistics demonstrate that the largest sums confiscated have resulted from criminal proceedings for ML, drug trafficking, OCG participation and tax crimes. The EUR 50 million figure between 2015 and 2021 is commendable, but with the number of potentially proceeds generating offences committed in that period, and noting the spike caused by one case from 2015, it is fair to question whether the overall figures adequately correspond to the risks.

335. As noted above, there is no breakdown between domestic and foreign offences, hindering the ability to assess the results against risks. It is not clear that Estonia is proactive in pursuing assets, whose provenance is criminality in Estonia, which have left the jurisdiction, hence the discrepancy between estimated laundered sums and sums actually confiscated. A limited number of records kept on confiscated property which is actually recovered is also a deficiency which restricts the review by the AT.

336. The results do, however, demonstrate a commitment to target the proceeds of crime, at least when located in Estonia, which is largely consistent with the national policies and priorities referred to in core issue 8.1. Cases such as Third-party ML (see IO.7) are to be highly lauded. As discussed above, there have been some examples of seizing and confiscating VAs which is positive, yet the results are not consistent with the risks associated with this sector.

Overall conclusions on IO.8

337. In conclusion, Estonia has demonstrated to some extent that it is effectively confiscating criminal property (primarily extended confiscation or property of an equivalent value) when the assets are in Estonia, and they achieved some reasonable results. Whilst the headline figure of 50 million EUR in confiscated assets is not insignificant, the overall seizure and confiscation results appear to be modest comparing to the country's estimation of domestic proceeds, as well as assets which have left the jurisdiction. The limitations in the statistics (breakdown between domestic and foreign, underlying predicate offences, property recovered) hinders the authorities' ability to accurately assess the achieved results and take appropriate steps for the improvement of the system. The LEAs appear well resourced to cope with the demands of pursuing criminal assets, the legislative framework is robust and there is a political and operational commitment to pursue confiscation as a policy objective. There are deficiencies as regards the lack of declaration system for intra-EU cash and BNI movements and for mail and cargo, yet the authorities do appear to be nonetheless thorough in searching passengers, visitors, mail or cargo in any event for suspicious cash and/or goods.

338. **Estonia is rated as having a Moderate level of effectiveness for IO8.**

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

a) In Estonia, there has been one successful TF prosecution and conviction related to collecting and providing funds to support FTFs, who have been recognised as threat. Nevertheless, given the other inherent TF vulnerabilities identified by the authorities, the achieved result does not fully correspond to the risk profile of the country. In addition, deficiencies in TF risk understanding (see IO.1) affect the overall effectiveness.

b) There have been five criminal TF investigations in Estonia. Features of these cases indicate authorities' skills and knowledge to deal with TF offence. Authorities uses a range of sources and investigative techniques when identifying and investigating TF, yet EFIU disseminations and terrorism related offences alongside with financial investigations could be exploited more in order to determine potential TF offences.

c) Authorities advised that they follow the internal guideline for conducting TF investigations. The guidelines lack comprehensiveness in terms of addressing identified challenges in investigating TF offence especially when VASPs and NPOs are concerned, as well as conducting financial investigations.

d) In Estonia, there are several counter-terrorism strategies: Internal Security Strategy (STAK) 2020-2030, Foundation of Estonia's fight against terrorism from 2013 and EU Policy and Priority 2015-2019. Among those, features of TF investigations (threat posed by FTFs) have been integrated to some extent in STAK 2020-2030. None of the TF investigations initiated so far supported national designation.

e) The sanctions applied in the TF conviction are not effective , particularly when compared with the sanctions applied for other serious offences.

f) In cases where it was not possible to determine a TF offence, Estonian authorities have used alternative measures such as revocation of visas, residence permits and e-residency and expulsion of natural persons from the country.

Immediate Outcome 10

a) Estonia implements the UN TFS without delay. The UN TFS is mandatory for enforcement in Estonia from its adoption date. Estonia uses both mechanisms for these purposes: the EU and domestic.

b) The mechanisms for designation of persons and entities under the UN TFS framework at the domestic level or internationally were not developed over the majority of the assessment period. No formalised approach was ensured to the designation process, including discussions and decision taking within the scope

of a formal fora, although there are convictions achieved and other circumstances are present to give raise to a more focused and formalised consideration of the subject.

c) Estonia has increased its attention towards implementation of international sanctions by the OEs over the latest period. So was confirmed by the actions of the supervisory authorities. While more enhancements are required, the EFIU improved timeliness of communication of UN TFS. The supervisors developed and published guidelines on implementation of TFS by the OEs in 2021 (EFSA) and in 2022 (EFIU), but some sectors are not adequately covered. Overall, the OEs demonstrated to have understanding of the UN TFS and other international sanctions but remain confused in applicable regimes. A stronger performance was demonstrated by the FIs as compared to VASPs and the DNFBPs. The VASPs have noted that considering the specificities of their provided services more adapted guideline is required.

d) Estonia conducted risk assessment of the NPO sector within the framework of NRA in 2021 and a separate study in April 2022. While the NRA was focused at assessing the TF threats and vulnerabilities in the NPO sector in general, the second study aimed at detection of the subset of NPOs that are vulnerable to the TF abuse. These efforts of authorities are commendable, but major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including identification of the specific subset of the NPOs, *inter alia* through analysis of a wider input data and expansion of the scope of considerations. More efforts are required also at the policy making, institutional and legislative levels.

e) Overall, there are important deficiencies in the understanding of TF risks by the Estonian authorities. This respectively affects the adequacy of measures taken for implementation of the TF–related UN TFS and prevention of the abuse of NPOs for TF purposes.

Immediate Outcome 11

a) Estonia implements the UN TFS without delay. The UN TFS is mandatory for enforcement in Estonia from its adoption date. Estonia uses both mechanisms for these purposes: the EU and domestic. UN TFS on PF were not communicated to the OEs. Respectively, the OEs were informed about the designations and amendments to those when decisions were made within the EU legislative framework.

b) Overall, the OEs demonstrated to have understanding of the UN TFS and other international sanctions. Among the FIs, banks and among DNFBPs, notaries demonstrated higher level of knowledge and performance. The OEs, especially the weaker sectors when discussing the TFS sanctions did not display being especially aware of the specificities of the UN PF-related sanctions. The ability of the OEs to detect a BO can potentially impact detection of funds or assets, especially when owned indirectly.

c) Over the last year Estonia reinforced its attention towards the implementation of the TFS measures, and demonstrated tangible progress also in supervisory

efforts, primarily focusing at the most important sectors, banks and VASPs, for which Estonia should be commended.

d) The country has a developed framework for the counter - proliferation matters within the scope of the SGC. These measures also contribute to prevention of financing of proliferation.

Recommended Actions

Immediate Outcome 9

a) Estonia should ensure that TF activities are investigated and prosecuted in line with its improved understanding of national TF risks.

b) Estonia should regularly carry out financial investigations when investigating terrorism and other related cases (e.g., trafficking of arms, drugs, human etc.) with a view to identifying and investigating potential TF offence.

c) The ISS should broaden the scope of its guidelines on identification and investigation of TF cases by integrating measures on (i) conducting parallel financial investigation in terrorism related offences; (ii) detecting and investigating TF with respect to activities of NPOs and VASPs. Estonia should develop and provide the LEAs with a guideline on conducting parallel financial investigation for identification of TF when investigating other related offences (e.g., trafficking of, arms, drugs, humans etc.).

d) Estonia should develop guidance or other mechanisms (such as trainings) in order to ensure that sanctions applied in TF cases are effective.

e) Estonia should improve existing counter terrorism strategies based on the emerging risks as well as on the outcomes of the ongoing investigations.

Immediate Outcome 10

a) Estonia should ensure considering designations according to UNSCR at the domestic and international level collectively, in the formal fora, including formal consideration of whether the UN designation criteria are met with respect to persons under investigation or convicted, also irrespective of existence of criminal proceedings.

b) Estonia should further improve the reporting of OEs under the UN TFS regimes, including by enhancing the OEs' knowledge of the UN TFS, providing more granular sector specific guidance to OEs, *inter alia* to VASPs and DNFBPs (especially CSPs and casinos). Additional outreach shall be provided to OEs, especially the sectors with a weaker knowledge and capacity.

c) Estonia should widen its understanding of TF risks in the NPO sector and enhance the identification of the NPOs most vulnerable to potential TF abuse, through analysis of a wider input data and expansion of the scope of considerations. Estonia should take adequate measure to ensure transparency and accountability of NPOs, effective risk-based supervision, set and apply effective sanctions, develop and provide guidance and outreach, especially targeting the higher risk NPOs.

d) The EFIU should ensure regular communication of new designations and amendments to UN TFS on TF to OEs immediately upon taking such action.

Immediate Outcome 11

a) Estonia should improve understanding of UN TFS regimes by the OEs, the knowledge of their obligations and implementation of those. Authorities should provide more granular sector specific guidance to OEs, inter alia to VASPs and DNFBPs (especially CSPs and casinos). Additional outreach shall be provided to OEs, especially the sectors with a weaker knowledge and capacity.

b) Estonia should continue strengthening its institutional capacities for effective supervision of implementation of UN TFS measures and ensure that the implementation of PF TFS by all OEs is regularly monitored.

c) The EFIU should ensure regular communication of new designations and amendments to UN TFS on PF to OEs immediately upon taking such action.

339. The relevant IOs considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

4.2. Immediate Outcome 9 (TF investigation and prosecution)

340. The ISS is a competent authority to identify and investigate terrorism related offences including TF. It is also responsible for intelligence gathering, prevention and mitigation of terrorism and TF threats. The GPO has a specialised prosecutor dedicated for TF investigations and prosecutions. The Criminal Courts have jurisdiction over terrorism and TF cases.

4.2.1. Prosecution/conviction of types of TF activity consistent with the country's risk-profile

341. Estonia conducted NRA and assessed TF threat level as generally low, except when it comes to the financial sector which is assessed as average, and high in the domain of VAs (see IO.1). The country's vulnerability is, as it is stated in the NRA and elaborated by the authorities, above average in the non-profit sector amid religious associations and charity organisations, as well as in the financial technology sector among crowdfunding service providers. Moreover, authorities estimated that around 20 individuals associated with Estonia have been or remained in conflict areas in the Syrian-Iraqi zone. In 2019 the ISS identified nearly 50 individuals linked to Islamic extremism or terrorist organisations either arriving in or travelling through Estonia.[154] It can be understood that authorities do recognise the threat posed by FTFs and propensity of individuals to move funds, while "raising" and "using" funds for TF purposes are considered to be improbable activities to happen in Estonia. Overall, as described in IO.1 there is a need for further efforts toward appropriate identification and reliable assessment of TF risks in Estonia.

[154] ISS Annual Review 2019-2020, p.41-42.

342. There has been one TF conviction achieved against two natural persons in Estonia. No other case has been prosecuted so far for the TF offence.

Box N°4.1: TF conviction

In 2017 two Estonian residences, (Ramil Khalilov and Roman Manko) were convicted for terrorist financing offence committed in 2013. Investigation was launched based on the ISS intelligence and defendants were charged for providing funds (money and airplane tickets) to another Estonian resident Sazanakov who travelled from Estonia to Syria to join terrorist organisation. Khalilov bought tickets for Saznakov and gave him instructions how to reach destination. Furthermore, he gathered money in Estonia in the amount of EUR 500, out of which EUR 400 was provided by Manko who additionally tried to support Sazanakov by travelling to country L to collect money. Even though there was a bank account open in foreign country for providing financial support for Saznakov, collected money was delivered in cash by Khalilov who travelled to Syria with Sazanakov's wife and child, also facilitating their trip to Syria. The ISS carried out financial investigation e.g., bank inquiries, mapping of assets etc.

Khalilov and Manko were sentenced to three and two years of incarceration respectively for terrorism financing offence.

343. It can be concluded that so far achieved results commensurate with TF risk in Estonia to some extent. Undoubtedly, presented conviction is a good example, showing efforts and skills of the competent authorities to successfully and timely investigate, prosecute and convict TF offence even when negligible amount of money or other funds were used to support terrorist activities. This conviction addresses some of the TF threats in Estonia, i.e., it involves criminal activity of collecting funds within the country and sending it in cash to a conflict zone to support FTFs. While FTFs have been recognised as a threat, authorities assessed that the phase of collecting funds is unlikely to occur in Estonia since they emanate from foreign jurisdictions and just go through the country (moving phase). In addition, no prosecutions or convictions have been achieved in the other areas identified as vulnerable, such as NPO and VAs.

4.2.2. TF identification and investigation

344. When identifying TF, the ISS looks at the various of sources such as (i) internal intelligence; (ii) information from foreign counterparts; (iv) information from domestic LEAs, including the PBGB database; (v) EFIU disseminations, etc. The ISS analyses financial patterns and transactions, independently and in cooperation with the EFIU. The focus is on the phase of "movements" of funds to and from high-risk jurisdictions, that are used to support terrorist activities, organisations, and individual terrorists. Once they collect enough evidence during the course of intelligence-based investigation, a criminal investigation is launched.

345. The ISS has advised that they use internal guideline when conducting criminal TF investigations. The main features of the guideline were presented to the AT, and it can be concluded that while being a useful tool, it lacks comprehensiveness to tackle sophisticated TF activities, especially when VASPs and NPOs are abused. In addition, there is no instruction how to conduct financial investigations in terrorism related offences, which would enable LEAs to detect potential TF. Notwithstanding, based on the case examples, it is evident that the ISS uses a range of investigative techniques to collect evidence when investigating TF offence such as: phone interceptions, social media scrutiny, checks against targeted financial sanctions, collecting evidence from foreign jurisdictions, conducting financial analysis.

346. Over the period under consideration, there were 51 intelligence investigations conducted by the ISS to identify potential TF offence. One of the examples that can be disclosed is investigation of the 13-years old Estonia national, member of the terrorist organisation FDK which intended to carry out a terrorist attack and tried to recruit members via internet. Authorities explained that they used various techniques in order to identify TF (checking phone calls, incomes, his expenses and expenses of related persons, his activities) and concluded that minor was self-radicalised, and no support was received from any other person.

347. There were five criminal TF investigations initiated so far in Estonia. Four criminal investigations are ongoing (which cannot be included in this report for reasons of operational sensitivity) and one case is successfully convicted (see Box N°4.1). Details of those criminal investigations were discussed with the country. It was demonstrated that, authorities used a variety of investigative measures (among others, collecting evidence from FIs, foreign countries, hearing witnesses, using secret surveillance measures). It appeared that the main impediment to conclude some of those investigations was the lack of possibility to hear defendants, as well as to collect certain evidence from conflict zones.

Table N°4.1: No of intelligence-based investigations lead by the ISS

Year	2015	2016	2017	2018	2019	2020	2021	Total
No. of cases	3	4	2	5	9	12	16	51

348. Whilst presented practice indicates professionalism and commitment of the competent authorities to investigate TF offence, some concerns related to identification and initiation of criminal investigations remain, as explained below.

349. A number of reports have been filed by OEs to the EFIU and later disseminated to the ISS (see table under IO.6). However, only few of those reports were used for identification purposes (intelligence-based investigation) and just one triggered the criminal investigation. The high number of TF-related reports is explained to be a consequence of pure connection of transactions to high-risk countries. Even though the reporting system was improved in recent years and requires that the OEs file reports when there are in addition to a link to high-risk also one or more additional indicators[155] present, no changes in the outcomes of the reports have been seen (see IO.6).

350. Estonian authorities do not exploit the potential of initiating TF investigations when investigating terrorism related offences.[156] For example, trafficking of illegal arms and explosives are considered as crimes that borders with terrorism, and the ISS does not consider Estonia as a source, transit or destination country for illegal arms. Nevertheless, there are indications of weapons sold via black market in a number of European countries including Estonia.[157] While the authorities have explained that they have looked at TF aspects of the case, they did not demonstrate what specific steps have been undertaken and what aspects have been analysed in order to determine if proceeds and instrumentalities of this crime have been used to finance

[155] "Guidelines on the characteristics of suspicious transactions" p.20-21
[156] NRA section 3.2.2, MER Chapter 1, para 7.
[157] UNODOC, Illicit Trafficking in Firearms, their Parts, Components and Ammunition to, from and across the European Union, Regional Analysis Report, Vienna, 2020 p. 138-139. See also ISS Annual Review 2020-2021, p. 39-40, Iconprint/Tallinna Raamatutrukikoda, 2021.

terrorism. No indication whether financial investigations have been conducted in those potential terrorism related cases.

351. As noted under 9.1, VAs represents high TF vulnerability, especially considering the anonymity associated with services provided by VASPs. In the beginning of 2022, there were three VASPs with connection to Estonia listed on the OFAC sanctions list. The companies were connected to Darknet transactions and ransomware attacks.[158] Authorities indicated that at least one of the companies had clients from high-risk countries and clients connected to terrorism and FTFs. The ISS only broadly reflected on the subject suggesting that they did not find any criminal aspects of TF in Estonia, and therefore the firm conclusion cannot be made whether all aspects of the case have been analysed.

352. The same conclusion can be made regarding an investigation on cryptocurrency transactions (see case example). The investigation was launched based on an international request sent to the EFIU regarding a foreign individual carrying out numerous international financial transactions related to cryptocurrencies. It was believed that this activity was related to the financing of an Asian terrorist organisation. The ISS discovered FTFs among the clients of VASPs and except from the general description of the case and steps undertaken, the ISS did not demonstrate investigative methods used to detect potential TF in this specific area.

Box N°4.2: TF suspicions in cryptocurrencies transactions

In January 2018, the EFIU received an information request from a foreign FIU which concerned a foreign individual carrying out numerous international financial transactions related to cryptocurrencies. It was believed that this activity was related to financing of an Asian terrorist organisation. The EFIU received a cross-border dissemination on the suspicious transactions in total worth around EUR 70 000. The EFIU also received reports about suspicious transactions. The analysis was later disseminated to a foreign FIU. The ISS analysed the money transfers via Estonian financial institutions but found no suspicion of TF activities.

353. During the assessment period 4 MLA requests were sent to Estonia on terrorism-related cases and none of them triggered a domestic investigation. In addition, in 2016, Estonia extradited an Estonian citizen to a foreign country who was suspected of participating in a terrorist organisation. The ISS advised that intelligence investigations have been conducted, yet no detailed information was provided to assess the effectiveness of such procedure.

4.2.3. TF investigation integrated with –and supportive of- national strategies

354. TF investigations are, to some extent, integrated into and supportive of Estonia's national counter-terrorism strategies. Estonia indicated several strategic documents dealing with CFT issues.

355. The authorities introduced Internal Security Strategy (STAK) 2020-2030 as the main strategy document dealing with TF issues. STAK outlines the return of the FTFs to Europe, the growing number of individual terrorists, and online radicalisation, as key threats. Nevertheless, the STAK strategy is on a general level, stating the need for increased capacity to identify terrorist

[158] https://sanctionssearch.ofac.treas.gov/Details.aspx?id=36025, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=33855, https://home.treasury.gov/news/press-releases/jy0471, https://home.treasury.gov/news/press-releases/jy0701

risks and to combat threats for possible terrorist attacks and their consequences.[159] All TF investigations led so far in Estonia relate to collecting funds to support FTFs and those features are incorporated generally in the strategy. However, the Strategy does not contain provisions that would tackle the TF vulnerabilities, including related to collecting and moving assets and the legislative gaps that limit the TF criminalisation to better support the authorities' efforts in combating TF.

356. "The Foundations"[160] of Estonia's fight against terrorism is setting the goals of the fight against terrorism in Estonia. It is approved by the Government in 2013 and covers CFT in general terms, mainly by focusing on awareness raising needs among FIs, strengthening national and international cooperation and points out the importance of a solid understanding and assessment of threats of TF. Since this document has been adopted in 2013, it cannot be concluded that succeeding criminal investigations (including the one dating from 2015), were integrated with, and used to support, national counter-terrorism strategies and investigations.

357. Estonian authorities advised that EU strategies such as European Union Policy and Priorities 2015-2019 are also to be used as counter-terrorism policies for Estonia. However, the Policy does not reflect specific and comprehensive actions concerning TF, nor reflects on specificities of the national threat and vulnerabilities.

358. In addition, several other national strategies have been suggested by the authorities as being national TF strategies such as: the "Estonia 2035" development strategy, The Estonia 2035 Action Plan, Fundamentals of Criminal Policy until 2030, and the Anti-Corruption Action Plan 2025. Nonetheless, specific measures directly related to TF are not part of those documents.

359. As elaborated under 9.1 there has been one TF conviction and five TF criminal investigations in Estonia. This raises concerns since they were not used to support designations of terrorists and terrorist organisations, as described under IO.10.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

360. The sanctions provided in the Penal Code for TF offence appear to be proportionate and dissuasive (see R.5), but the practice demonstrates that the applied sanctions are not effective. This is demonstrated through the conviction of 2 persons under the TF criminal case where the first instance court imposed a sentence of 7 and 5 years of imprisonments and the Supreme Court lowered the final sentence to 2 and 3 years of imprisonment respectively. Those applied sanctions when compared with the sanctions imposed in other serious cases do not appear to be effective.

4.2.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

361. The authorities have indicated that several alternative measures have been used in cases where it was not possible to determine a TF offence. Those include the revocation of visas, resident permits, e-residency, and the expulsion of some natural persons. The Estonian authorities have banned 22 persons from entering the country based on their connections to

[159] Internal Security Strategy 2020-2030, Ministry of the Interior.
[160] Foundations of Estonia´s fight against terrorism, 2013, Government of the Republic

jihadist terrorism and in all cases foreign counterparts were informed enabling them to identify and scrutinize possible future TF cases.

Overall conclusions on IO.9

362. In Estonia, there has been one TF conviction achieved so far, showing the authorities' ability to investigate, prosecute and convict for TF offence. Given the other inherent TF vulnerabilities identified by the authorities, the achieved result does not fully correspond to the risk profile of the country. Additionally, there are deficiencies in the assessment and understanding of TF risk as described under IO.1 which hinders overall effectiveness of suppression of TF. Though the ISS pursued criminal investigations for TF offence related to supporting of FTFs, there is a need to improve awareness of the authorities about other TF activities that could be further investigated.

363. TF investigations are integrated into the national strategies to some extent, but never used as basis to propose designations of terrorist and terrorist organisations. Criminal sanctions applied in practice are not effective. There are number of alternative measures applied in Estonia when TF conviction is not possible.

364. **Estonia is rated as having a Moderate level of effectiveness for IO9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for TF without delay

365. Estonia implements targeted financial sanctions (TFS) against TF pursuant to UNSCRs 1267/1989 and 1998 without delay. Estonia relies on both, domestic and the EU legislative frameworks. The legislative framework introduced in 2017 ensures enforcements of decisions of the UN Security Committees for 1267/1989 and 1988 on introducing changes and amendments into the list of designated persons and arrangements through the requirement to implement those upon adoption by the UN. At the same time, as an EU Member State, Estonia also applies the EU Regulations as a mechanism for the implementation of those sanctions, after the UN designations are transposed into the EU legislative framework.

366. The domestic regulatory framework in this field is comprised of the International Sanctions Act (ISA), which in addition to the mechanism of enforcement of the UN sanctions in Estonia provides for a high-level outline of the powers of the Government, various ministries and bodies in respect to implementation of the respective UN Resolutions. The authorities had also adopted a "Guidelines for proposing the designation or removal of a natural or legal person, entity or body from the list of subjects of an international sanction" aimed at setting a respective mechanism. The effectiveness of those set mechanisms was not possible to assess as these were not yet applied by the authorities due to very recent adoption of the document (adopted on 17 March 2022).

367. The MFA is the coordinating body for implementation of international sanctions. It is the national designated body for making proposals for including to and removing persons and entities from the lists of UN Security Committees for 1267/1989 and 1988 or addressing the Government of Estonia for application of sanctions pursuant to UNSCR 1373.

368. Estonia has not identified individuals or entities to propose any designations to the UN Security Council Committees pursuant to UNSCR 1267/1989 and 1988, as well as has not initiated designation pursuant to UNSCR 1373 at the domestic level and at the EU level. This, even despite of convicting two persons (Ramil Khalilov and Roman Manko) for TF, conducting 4 ongoing investigations into TF (some lasting several years), being aware of persons who left Estonia for Syria, and persons related to Islamic state and terrorist organisations traveling through Estonia, as described in detail under IO.9.

369. The authorities stated that the two convicted persons were not considered for designation either at the domestic or international level, as they were charged with 2 and 3 years of imprisonment which in their view is a stricter and more adequate measure. In their views, this would more effectively prevent these two persons from conducting TF further, than proposing them for designation with UN. The authorities convincingly explained also that ISS had detailed overview of Manko and Khalilovs transactions and assets. At the same time, the authorities suggested to have some informal discussion on a possible listing of those between the ISS and the OPG, but no protocol was taken. This was not supported by further fact-based elaboration or other evidence to verify the statement. The authorities did not demonstrate seeing benefits in formalised discussion on the matters of designation. They added also that they are familiar with the UN mechanisms for designation of persons and entities at the international level but did not consider it reasonable or practicable to propose designations. The AT does not consider this approach to demonstrate that the system in place is effective.

370. Estonia has never received any request from foreign states for designation of persons or entities within the UN TFS framework. It also has not had any case where it was necessary to consider initiating delisting of persons or entities. Had it received a request, until 2022 there were no dedicated mechanisms set to apply these. The Government Guideline from March 2022 established the mechanism. The effectiveness of this was not yet possible to test but from the technical perspective it is sufficient.

371. The EFIU is the designated national authority for communication of designations to the FIs and DNFBPs. It does so through its website, using both mechanisms: providing a link to the general page of the UN Security Committees, and notifying about new designations and amendments to the existing information on persons or entities by publishing information in the form of the news. Analysis of the available data demonstrates that communication was lacking timeliness between 2020 and mid-2021 (with in average 5-6 days of delay). Since then, the overall picture had improved notably (mostly no delays occurred). In some few instances the designations and amendments were not published. While those delays did not have a practical effect on the OEs relying of the globally recognised electronic tools to have access to the updated designation lists, this had effect on the others.

372. When discussing with the OEs, the UN TFS sanctions were often mixed with other financial sanctions set at the supra-national level and by some foreign countries (UN, EU, OFAC, other). Overall, banks and some other FIs advised that since the last year the supervisory authorities attached more attention to implementation of financial sanctions. This was explained by the enhanced supervisory attention to implementation of the financial sanctions by the OEs, issuing two guidelines by the EFSA and EFIU respectively. The EFSA Guideline is addressed only to its supervised OEs. The EFIU Guideline is addressed to all natural and legal persons in general, and

to covered FIs, VASPs and legal service providers specifically. Hence, those together do not target all of the FIs and DNFBPs in a specific manner, to take into account the modalities of their respective services, as required by the FATF Standard. At the same time the VASPs have noted that considering the specificities of their provided services more adapted guideline is required.

373. The EFSA the CN and BA conducted trainings on implementation of international sanctions for their supervised OEs. Authorities suggested that during the on-site, on 28 April 2022, the EFIU has arranged an info-day, where it provided awareness on various sanctions regimes implemented by Estonia to VASPs. Other OEs did not confirm being provided with the awareness raising events or trainings with respect to implementation of the UN TFS. The communication with the EFIU is request-based. When approached, the EFIU provides a good support.

374. Among the FIs, Banks and other types of institutions that belong to the banking groups demonstrated sufficient understanding of UN TFS requirements, followed by the PSPs, the Consumer credit providers and the exchange services providers. The VASPs demonstrated varied level of knowledge. Among the DNFBPs, the awareness varied but was lower as compared with FIs. Notaries were the sector with a higher awareness. The CSPs, real estate service providers, lawyers and casinos were confused between various types of sanctions. Within the DPMS sector awareness of their freezing obligations varied considerably. Nevertheless, overall, most of the sectors were aware of the need to keep the lists of persons designated under various sanctions up-to-date, and when partial match arises, obtain additional information to confirm the possible match. Where not sure, the report shall be filed to EFIU.

375. The majority of the OEs confirmed to have available internationally recognised and widely utilised electronic tools for ensuring information on UN TFS is up to date. The Notaries are provided with the e-notary system that allows to automatically screen entries of persons or new transactions against UNSCR TFS. The EFIU analysis shows that third party service providers that are used by the VASPs for screening are not reliable in all cases and thus OEs are expected to adopt additional mitigating measures.

376. Majority of OEs could confirm they conduct screening of customers against UN TFS designations when onboarding the customers. Banks, other larger FIs, OEs that belong to banking groups and VASPs confirmed to perform also regular screening of the existing customers against the lists. Some mentioned that they do so more than 4-6 times per day. All the customer database, including the BOs of the customers are screened. The VASP had, nevertheless, highlighted that the implementation, in practice, of the travel rule would make it possible to conduct more appropriate screening of transactions as it is required for financial intermediaries, but it is impossible yet.

377. Most of the DNFBPs conduct a follow-up screening of customers less frequently. The period varies from weekly to yearly.

378. The identification of customers and the verification of customer data, as well as the identification and verification of the BO, is applied consistently across all sectors, but the quality varies (see IO.4). There is generally a more in-depth and dynamic approach in the banking sector. In contrast, the depth of understanding is more superficial outside this sector, with undue reliance on checks undertaken by other actors within the financial sectors.

4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations

379. Estonia estimates its TF risk in most of the fields as low, but it is heightened in respect to NPOs. The NRA estimates the TF vulnerabilities of NPO sector for TF to be at an average/high level. Estonia suggests that as in the case of ML, the TF vulnerabilities of the NPO sector are related to channelling funds through Estonia. At the same time fund raising and use of funds for TF are considered non-existent in Estonia. This conclusion, nevertheless, is not supported by the reliable analysis and data, and as demonstrated through analysis in IO.9, raises doubts. In addition, the NRA concluded that other vulnerabilities are related to the allocation of scarce resources to address the sector, low awareness, the lack of sector-specific guidelines, and the complexity of supervision, which is also observed by the AT, as described below.

380. Further to the NRA 2021, the ISS determined that 56 NPOs (3 foundations and 53 non-profit associations) are at a higher risk of TF. This understanding was explained in the "Overview of the Non-Profit Sector at a Higher Risk of Terrorist Financing" published in April 2022. While it is commendable that the country took steps for targeting specifically the subset of NPOs that are particularly vulnerable to TF, the used methodology and the entry data appeared to be rather limited. The authorities confirmed that a more comprehensive dataset and wider scope of considerations needs to be employed.

381. The analysis of the non-profit sector conducted by the authorities refers to 56 NPOs, within a total of more than 24 thousand such entities, which have been deemed by Estonian law enforcement authorities to be exposed to a higher risk of terrorist financing. At that, the report does not specify how exactly those 56 NPOs have been identified as the ones which, by virtue of their activities or characteristics, are likely to be exposed to a higher risk of TF abuse. Moreover, the report reflects – as much as relevant data is available to the authorities – on areas of activity of NPOs, their related parties (including non-residents), members and employees, turnover and assets, collection and use of donations, and cross-border payments in the context of all 24 thousand NPOs, with subsequent reference to respective data, where available, on the ones considered by the authorities as higher risk. Overall, the report does not seem to add much to the understanding of the TF risk in Estonia insofar as it does not reliably identify the NPOs likely to be at the risk of TF abuse; specify the nature of threats posed by terrorist entities to these NPOs and the ways in which they have been or could be abused by terrorist actors; review the adequacy of measures, including laws and regulations, that relate to the mentioned subset of the NPO sector in order to be able to take proportionate and effective actions to address the risks identified.

382. Authorities confirmed that so far, relevant policymakers and the supervisory authorities have not had enough resources to make the necessary commitment to the NPO sector. This was also acknowledged in the NRA 2021, with the mitigation measures proposed as strengthening the EFIU supervisory role and strengthening the reporting requirements of the NPO as an OE.

383. By the time of the onsite the authorities did not demonstrate yet revising their institutional and regulatory approaches to ensure proportionate and effective actions can be taken to those identified subset of NPOs falling under the FATF definition. Only recent amendments in the MLTFPA were recalled, which are related to monitoring of NPO transactions. The threshold of cash transactions for which the NPOs shall file a transaction report to EFIU was lowered and a requirement to do so also when higher ML/TF risk factors are observed added, i.e., treating the

NPOs as the OEs with limited obligations. This is a positive step towards improving the monitoring and detection of higher-risk transactions, and potentially improving the NPOs awareness and capacities to identify potential TF. This measure, nevertheless, was partly there for long time, while with a higher threshold, and did not prove bringing fruits so far. The NPOs also did not recall having contact with the EFIU and demonstrated to not be aware of their reporting obligations and the addressee of the report. This measure does also not suggest amounting to targeted approach towards 56 higher risk NPOs.

384. As concern the vulnerabilities observed by Estonia in the NRA, with respect to low awareness of the NPOs about the risks of TF abuse, it should be noted that while a sample of NPOs contributed to NRA by means of filling in questionnaires, those were not made aware of the outcomes of the NRA. Despite the NRA was published on the MoF website; the "Overview of the Non-Profit Sector at a Higher Risk of Terrorist Financing" was published on the EFIU website, social media and a press release was made; the EFIU suggested that it conducted training in October 2021 to present the NRA findings; none of the NPOs confirmed to be aware of those arrangements. This indicates that those steps taken did not amount to sufficient outreach to the NPO sector, especially a targeted approach to the NPOs identified as at higher risk of TF abuse.

385. The NPOs demonstrated not to have an understanding of what they should focus on to prevent abuse of their organisation for TF. The examples brought were that the NPOs try to examine their partners in foreign regions by mostly relying on already known partners but do not check on the transactions.

386. The NPOs confirmed not to have any guidance from the authorities on the ways they can recognise and prevent a potential abuse for TF and would welcome instructions and concrete typologies. Those, which are the part of international well developed NPOs suggested to follow the instructions and rules provided by the headquarters. There are also various NPO umbrella organisations operating in Estonia that have their own codes of ethics and rules for fundraising, but the analysis conducted by authorities suggests these do not contain measures to prevent the TF abuse.

387. NPOs rely on the banks executing transactions for verification of the NPO counterparts, including the BO of legal persons, where relevant. While banks seem to have sophisticated systems in place to monitor transactions, supervision showed that there were some deficiencies in CDD practices (see IO 3 and IO 4). Although banks put a credible and firm approach to servicing the NPOs, there are no additional checks performed by the NPOs which makes them blind towards the appropriate identification of their donors and beneficiaries.

388. As concerns the complexity of monitoring, it shall be noted that the ETCB is the authority designated for monitoring the financial activities of NPOs (with a disclosure of the recipients and donors of donations and grants). The process and the purpose, nevertheless, are purely aimed at the tax revenue controls – analysis of annual financial statements. While the ETCB suggested to apply a risk-based approach the provided description and the list of criteria used were related to detection of deficient tax declaration or tax avoidance cases and not criteria targeting the NPOs with higher TF risk exposure. On the basis of the examples, it was demonstrated that the ETCB inspections focused at tackling the ML risks, rather than on the prevention of TF risks.

389. In addition, the EFIU has a supervisory role over the NPOs as the OEs (as described above). So far, the EFIU had conducted supervision in 2015, targeting the NPOs under ML/TF risk.

Nevertheless, it turned that the selected subset had not carried out cash transactions of EUR 10 000[161] and above, that would have made them subject to the MLTFPA, and hence subject to the EFIU competencies. No other supervision was conducted since then.

390. As concerns the BR, it registers the NPOs applying equal proceedings as to legal persons. BR conducts formal checks of the appropriate submission of documents and as a subject to screening proceedings against the UN TFS lists, checks the persons against the sanctions lists. For the NPOs, these shall be information on Board members, statute and a phone number of a representative. The BR is registering the board members of the NPO online and conducts basic verifications through the checks with the population registry. Where the board member is not Estonian the registration shall be conducted through the Notary. The BR fully relies on the checks made by the Notary. Another disadvantage is the lack of appropriate controls with the e-residents applicants. In addition, the NPOs must register their BO in the BOID. The BR conducts periodical checks for detecting the change in the registered data - every 3 years it is checking the Board members. Otherwise, this comes to its knowledge when the NPO reports. Hence, in terms of timely monitoring of changes, hence the accuracy and currency of information is questionable. The absence of effective sanctions for not providing adequate data to the registry, and the circumstance that the absence of an annual activity report cannot be sanctioned effectively hinders the reliability of the Estonian business registry in general and with respect to NPOs, specifically. The issues with the quality of registration and conducted checks and applied sanctions is analysed in detail under IO.5.

4.3.3. Deprivation of TF assets and instrumentalities

391. Estonia demonstrated that overall, the system in place would allow to freeze and deprive the TF assets when identified within the scope of the UN TFS. So far, no positive match with the UN TFS had been detected. As concerns other mechanisms, the application of these are described under IO.8 and IO.9. So far, there were no TF assets deprived, since there was no confirmed occasion.

392. Estonia has never received any request from foreign states for freezing of assets of persons or entities designated within the UN TFS framework. Had it received a request from the EU Member States, the EU legislative framework would be applied. With respect to the scenario of non-EU Member State request, there were no appropriate, formalised mechanisms set during most of the assessment period up until 17 March 2022, when the Government Guideline was adopted.

393. Estonia has not had any case where it was necessary to unfreeze assets or provide access to frozen property under the UN TFS regime. When discussing this matter the authorities demonstrated some, but not adequate knowledge of various modalities for calling into life these procedures, when they would occur. This was primarily being an impact of the long-standing deficiencies in the domestic regulatory framework and the lack of formalised and detailed procedures.

[161] Until amendments of 15 March 2022 to the MLTFLA, threshold of transaction reporting requirement for NPOs was set at the level of EUR 10 000.

394. As concerns the performance of the OEs with respect to identification of possible assets for freezing at the domestic level, the statistics below reflect on the overall numbers of the detected matches, which turned to be false positive. These represent the total number of reports filed by OEs on international sanctions, per the listed year. These include UN TFS, EU, and other foreign country-sanctions that Estonia had chosen to follow.

395. Among the OEs, those reports were filed by the banks, VASPs, notaries, DPMS, PSPs, investment firms and securities sector, real estate, MVTS, consumer Credit companies, casinos and auditors (per order of the reporting). The banking sector was the major contributor, followed by the VAPS sector, which had an input over the last two years.

Table N°4.2: Total number of international sanctions reports filed by OEs

	2015	2016	2017	2018	2019	2020	2021
ISR	16	12	31	13	89	51	99

396. At the same time, the authorities specifically presented the figures for the detected false positive matches with the UN TFS. Banks and the exchange service providers demonstrated being especially vigilant to this matter.

Table N°4.3: False positive matches with UN TFS on TF and funds frozen[162]

	2017		2018		2019		2020		2021	
Types of OEs	ISR on UN TFS	ISR on false positive matches /funds suspended for UN TFS	ISR on UN TFS	ISR on false positive matches /funds suspended for UN TFS	ISR on UN TFS	ISR on false positive matches /funds suspended for UN TFS	ISR on UN TFS	ISR on false positive matches /funds suspended for UN TFS	ISR on UN TFS	ISR on false positive matches /funds suspended for UN TFS
Banks	1	1/EUR 20	0	0	0	0	1	1/EUR 29,70	14	14/EUR 2963,50
Currency exchange service	0	0	0	0	0	0	1	1/EUR 20,16	0	0
Other OEs	0	0	0	0	0	0	0	0	0	0

397. The OEs explained that in all instances, when their operated system flags up a match with international sanctions, these transactions are analysed by the institution manually. These transactions undergo an enhanced scrutiny. Information on the persons concerned is verified against various independent sources. Where uncertainties remain, the OE files a report to the EFIU and suspends the transaction until the feedback from the EFIU. Estonian legislation allows for 30 days (with further extension) of suspension of transaction, so that a comprehensive analysis can be conducted also by the EFIU.

398. Banks were firmly aware, and also in possession of internal guidelines on how unfreezing would happen. Lawyers and notaries, and most of the DNFBPs stated that in a case of freezing of assets they would not take any steps towards unfreezing those until the EFIU instructs them to do so. The NPO were not aware about their freezing obligations under the UN TFS, and that the reports should have been filed with the EFIU. Hence it can be concluded that while the capacities

[162] No information is provided in the table of positive matches since there were not such.

vary from sector to sector, overall, where the case occurs, the OEs are in a position to take respective steps to ensure that the designated persons are deprived of assets.

4.3.4. Consistency of measures with overall TF risk profile

399. Overall, there are important deficiencies in the understanding of TF risks by the Estonian authorities. This respectively affects the adequacy of measures taken for implementation of the TF–related UN TFS and prevention of the abuse of NPOs for TF purposes.

400. Concerns with deprivation of assets of terrorists exist in respect to missed opportunities for designating persons as described above. The implementation of the TFS was significantly strengthened only from the end of 2021 as a result of the legislative amendments, publication of guideline for the OEs, and higher than ever attention attached to this topic in the light of the global developments, though, not directly related to the UN TFS framework. Nevertheless, some important technical issues still need to be fixed. This, especially being related to the level of a supervisory attention, need for improvement of the guidance and enhancement of outreach to OEs, ensuring regularity of timely communication of designations and amendments to the OEs, and performance on reporting ISR over the preceding years. While the authorities recognise that Estonia is used as a transit country for ML purposes, they do not demonstrate the understanding, that the same vulnerabilities of the OEs, especially the financial sector can be exploited for the TF purposes, or do not demonstrate how would this differ for the TF.

401. With respect to the NPO sector, the AT acknowledges the efforts of the authorities to conduct risk assessment within the framework of the NRA in 2021, which was followed by the "Overview of the Non-Profit Sector at a Higher Risk of Terrorist Financing" April 2022, but the quality of those is to be considerably improved. The consistency of applied measures to suggested risks was not yet demonstrated since both exercises detected a number of serious gaps in the capacities and attention of the authorities to the topic over the whole past period of time, and these were conducted only very recently.

Overall conclusions on IO.10

402. Estonia implements the UN TFS without delay. The mechanisms for designation of persons and entities, under the UN TFS framework were not developed over the majority of the assessment period. No person is designated either domestically or proposed to the UN, although there are convictions achieved and other circumstances are present to give raise to a more focused and formalised consideration of the subject.

403. The OEs have overall understanding about the UN TFS and other international sanctions regimes but remain confused in applicable regimes. Overall, a stronger performance was demonstrated by the FIs as compared to VASPs and the DNFBPs. Knowledge, performance and support to the important sectors, such as VASPs, and CSPs are a matter of concern. Attention to the subject matter was reinforced only since 2021.

404. Estonia conducted risk assessment of the NPO sector within the framework of NRA in 2021 and a separate study by the EFIU in April 2022. These efforts of authorities are commendable, but major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including in identification of the specific subset of the NPOs, *inter alia* through analysis of a wider input data and expansion of the scope of considerations. The risk-based preventative

measures with respect to NPOs are to be considerably improved. Hence, the consistency of measures in place for implementation of UN TFS and prevention of NPOs from TF abuse are adequate only to some extent.

405. **Estonia is rated as having a Moderate level of effectiveness for IO.10.**

4.4. Immediate Outcome 11 (PF financial sanctions)

406. While not presently required under the FATF Standards, Estonia conducted an initial assessment of its PF risks within the scope of NRA 2021. This exercise contributed to the authorities' understanding of the potential PF threats and vulnerabilities for Estonia. It was concluded that as concerns the PF threats, there are two directions that can be distinguished as more important for Estonia: breach of the sanctions regime through possible WMD transit using Estonian territory or companies established in Estonia; and evasion of sanctions through the VASP sector.[163] As regards the general vulnerability for PF, this would be potentially related to detection of a BO of a legal person, where it is a designated person. The general vulnerability was assessed at the level of low-average for Estonia[164].

407. Estonia has introduced mechanisms to implement TFS against proliferation, as well as control measures to identify possible cases of the circumvention of sanctions or of the inspection regime for exports of dual-use goods that proliferation networks may seek to exploit.

408. Trade relationships between Iran and Estonia are estimated from around EUR 5.32 million in 2017 to EUR 3.7 million in 2021 in imports. Trade with Iran focuses on export or import of fruits, nuts, food products, wood and peat.

409. Trade relations between Estonia and DPRK are close to inexistency as there was only one transaction conducted with DPRK in 2016 over USD 15 000.

410. In Estonia, E-residents from Iran have founded 132 companies, of which 25 were active at the time of the on-site. There were also two e-Residents from North Korea and one company (in the field of IT) established as of January 2022. The authorities advised that before going operative, this company was removed from the Estonian registry. Authorities suggested that the applicants for the e-residency program are scanned against the UN lists of designated persons. Overall, the vulnerabilities related to the implementation of the E-Residency Program (e.g., background checks), as also described in the other parts of the report, heighten the risk of evasion of international sanctions.

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

411. The legal framework provides to Estonia grounds for implementing UN TFS against PF without delay since 2017 by the adoption of the Government decision N156. This decision is adopted on the basis of the International Sanctions Act[165]. Both legal acts use a neutral language and apply to TF and PF-related UN international sanctions identically. This legislative framework

[163] NRA 2021, "Analysis of proliferation financing risks", p.3
[164] NRA 2021, "Analysis of proliferation financing risks", p.7
[165] The ISA was first adopted in 2010 and after undergoing 6 amendments, and was repealed by adoption of the new ISA in 2020.

ensures enforcements of decisions of the UN Security Committees through the requirement to implement those upon adoption by the UN.

412. At the same time, as an EU Member State, Estonia also applies the EU Regulations as a mechanism for the implementation of those sanctions, after the UN designations are transposed into the EU legislative framework.

413. Unlike the one with respect to the sanctions on DPRK, so far, in practice, the EU legislative framework ensures timely implementation of measures related to sanctions regarding Iran, since the list of individuals and entities is wider in the EU framework. In addition, there are supplementary mitigating measures applied by the EU requiring prior authorisation of transactions with designated Iranian entities. This allows the authorities to determine if the transfer of funds for which the authorisation is requested is permissible according to the EU Regulations.

414. Considering that the ISA applies equally to TF and PF related UN TFS, the institutional framework and the powers are identical to what is described under IO.10. The MFA is a coordinating body for implementation of sanction regimes and the EFIU is the designated body that is responsible for ensuring implementation of financial sanctions.

415. Unlike the TF-related sanctions, designations and amendments to the UN TFS on PF, were not communicated to OEs. This was also recognised by the authorities. Respectively, the OEs were informed about the designations and amendments to those, when decisions were made within the EU legislative framework.

4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions

416. There were no funds or assets frozen in Estonia pursuant to UN designations related to PF. The authorities suggested that over the period of assessment there were two instances when false positive matches with the UNSCRs on PF were detected. One was detected by a bank in 2018. This was a partial match with the name of a person in the UNSCR 1737 (2006). EUR 20 was suspended. On the other occasion, the BR detected a partial match with a person in the UNSCRs 1718/2006 and 1874/2009. It was a person nominated as a member of board for a company that applied for registration. In both instances the parties who detected the partial match conducted additional checks and submitted ISR report to the EFIU. The latter gathered additional information and conducted additional checks. The feedback was provided to the parties filing the reports in the form of the outcome of the EFIU analysis confirming that the matches were false positive.

417. So far, there were no occasions for triggering investigations and prosecutions related to PF in Estonia, but the country provided examples of two investigations into proliferation resulting in the denial of an export license.

418. The country has a developed framework for the counter - proliferation matters within the scope of the SGC. In addition, the MFA occasionally updates the AML/CFT Committee on implementation of, *inter alia*, the UNSCR 1540 on the prohibition of weapons of mass destruction, as well as on measures to control export of dual-use and military goods (see also IO 1).

419. Estonia has developed a National Strategy for the non–proliferation of weapons of mass destruction aimed at ensuring improvement of coordination of the existing systems for

suppression of WMD, strengthening the capacities for collection, exchange and analysis of intelligence data necessary to detect, identify and monitor threats caused by WMD and associated dual–use and military–use items. These measures, also contribute to prevention of financing of proliferation of these goods.

4.4.3. FIs, DNFBPs and VASPs' understanding of and compliance with obligations

420. In general, the framework as already analysed in detail under IO.10 applies also here. Hence the strengths and weaknesses of the system are the same. Among the FIs, Banks and other types of institutions that belong to the banking groups demonstrated sufficient understanding of UN TFS requirements, followed by the PSPs, the Consumer credit providers, and the exchange services providers. The VASPs demonstrated varied level of knowledge. Among the DNFBPs, Notaries were the sector with a higher level of awareness. The CSPs, real estate service providers, lawyers and casinos demonstrated a lower level of knowledge and within the DPMS sector displayed awareness varied considerably.

421. The OEs, especially the weaker sectors when discussing the TFS sanctions did not display being especially aware of the specificities of the UN PF-related sanctions. They had in general described measures they take to detect the matches and the following steps of additional verification of a transaction and related subjects, methods for filing the report to the EFIU and freezing assets.

422. The majority of the FIs, VASPs and some DNFBPs, especially notaries had suggested regularly screening the customers against the UN lists of designated persons, including ongoing monitoring. Performance differs in the other sectors, especially by the DNFBPs as concerns the monitoring of customers, the period of screening regularity varying from daily to weekly and in some instances up to yearly.

423. The majority of the OEs confirmed to have available internationally recognised and widely utilised electronic tools for ensuring information on UN TFS is up to date. The e-notary system automatically screens entries of persons or new transactions against UNSCR TFS. Without these checks, transactions in the notaries field are impossible.

424. The VASPs use sophisticated technological tools to screen their clients and their transactions against UNSCR TFS lists. However, most of the VASPs raised concern that the non-implementation of the FATF travel rule makes a proper screening of transactions, as it is required for financial intermediaries, impossible. Some VASP follow the principle of adhering to the strictest regulations they face (they are usually operational in more than one country) and are waiting for the EU to pass sufficient regulations.

425. Overall, the ability of the OEs to detect a BO (as described in IO.4) can impact detection of potential matches with UN TFS, especially, when the assets are owned or controlled indirectly.

426. The EFIU (in 2022)[166] and the EFSA (in 2021) have issued respective Guidelines for implementation of financial sanctions. The EFIU Guidelines are addressed to all natural and legal

[166] At the later stage of evaluation, the EFIU suggested that there were preceding guidelines available for implementation of TFS measures, and the document from 2022 is the amendment to those. But preceding versions were not presented to the AT to verify.

persons in general, and to covered FIs, VASPs and legal service providers only, in particular. Hence, they do not extend specifically to all FIs and DNFBPs (including the CSPs and casinos) as required by the FATF Standard. The EFSA Guideline is addressed only to its supervised OEs.

4.4.4. Competent authorities ensuring and monitoring compliance

427. In Estonia, the EFIU is a designated authority for the state supervision over the application of financial sanctions. At the same time, the EFSA exercises supervision over compliance of application of financial sanctions by its supervised OEs. The TFS supervision of lawyers and notaries is carried out by the BA and the CN (the MoJ delegated its powers in line with the legislation). Other DNFBPs are subject to state supervision carried out by the EFIU over the application of TFS by natural and legal persons. The LEAs may also exercise state supervision over implementation of the financial sanctions.

428. The authorities provided statistics on supervision of implementation of TFS by OEs conducted by two authorities. The number of inspections conducted by the EFIU are provided in the table below. After obtaining supervisory competence over UN TFS compliance on 1 January 2021, the EFSA initiated 9 thematic on-site inspections on its supervised entities, within the same year. No information is available with respect to supervision conducted by other authorities.

Table N°4.4: EFIU supervisory inspections (including related to TFS)

	OEs	2015	2016	2017	2018	2019	2020	2021
Thematic inspections on implementation of TFS	**Total**	**1**	**1**	**3**	**0**	**1**	**3**	**13**
	VASPs	0	0	0	0	0	0	13
	Payment institution	1	1	3	0	0	2	0
	Banks	0	0	0	0	1	0	0
	Credit providers	0	0	0	0	0	1	0
Full scope inspection, including on implementation of TFS	**Total**	**61**	**73**	**43**	**6**	**19**	**27**	**18**
	Pawnshops	34	22	5	0	0	0	1
	Credit providers	8	25	1	1	5	1	2
	VASPs	0	0	0	3	5	6	13
	Dealers	6	10	6	0	1	3	0
	Currency Exchange	3	9	10	0	0	0	0
	Real estate brokers	0	0	0	0	8	10	0
	Accountants	0	0	16	0	0	0	0
	CSPs	0	4	4	2	0	2	2
	Casinos	6	1	0	0	0	0	0
	DPMS	3	2	1	0	0	0	0
	Auditors	0	0	0	0	0	5	0
	NPO	1	0	0	0	0	0	0

429. The EFIU described that inspections of compliance with implementation of TSF measures, *inter alia,* include checks on the organisational structure, staffing and knowledge, internal control rules, activities of the management board, technological solutions used to monitor business relationships, outsourced services, accuracy of the sanctions lists and other elements of functionality of the OEs. When inspecting VASPs, technological solutions are analysed in a greater detail, and OEs gave a detailed overview of the functioning of their systems. In addition to on-site inspections, the TFS measures are also inspected through off-site questionnaires. As a result of the inspections, the EFIU identified that the main shortcomings where related to the lack of procedures and internal controls. The EFIU analysis also showed that third party service

providers that are used by the VASPs for screening are not reliable in all cases and thus OEs are expected to adopt additional mitigating measures.

430. In 2019 EFIU has issued precepts for the elimination of deficiencies with a warning of a possible penalty if the OE failed to do so. The EFIU requested the OEs to present action-plans for elimination of detected deficiencies.

431. Notably, the EFIU's efforts over the last year were focused at VASPs, the sector with the higher ML/TF risk exposure, as was confirmed by the NRA 2021.

432. The EFSA has provided to the AT the methodology of the inspections and described the process of inspections conducted by it in the supervised OEs. The target group was the banking sector (more than 90% in assets), which was explained by the considerations of the EFSA about the ML/TF risk exposure of the selected entities (on products and services being offered, country where financial institution operates, customer database and size of the market). The scope of the on-site inspections included checks on: financial sanctions awareness; procedures and internal guidelines; application of preventative measures, including identification of BOs; systems and technology used for identifying subject to a TFS; effectiveness of the inspected entity's system. Inspection consisted of analysis of internal procedures, meeting with the management and the responsible officers, and sample testing to assess whether the systems and controls in place work in practise and are effective. Different scenarios were used for both the customer database and transaction screening testing (e.g., noise simulation, phonetic similarity, typing errors, spelling differences etc.).

433. The EFSA went beyond the inspection of the freezing requirements as per UNSCRs and had also inspected the capacities of OEs for detection of restrictions i.e., related to arms and related materials embargo, interdiction and transportation (sanctioned vessels).

434. Overall outcomes of the financial sanctions on-site inspections the EFSA conducted were as follows:

- use of correct and up-to-date external and internal sanctions lists should be improved;
- sanctions list based approach alone is not sufficient to ensure sanctions compliance, but it must be complemented by the implementation of EDD/CDD/SDD measures;
- financial institutions should be more aware of the sanctions regimes their clients may be exposed to;
- quality of processing sanction alerts should be improved;
- rules of procedure must be more proportionate and take into account the risks of sanction arising from the concrete business of the financial institution;
- internal controls must be improved to ensure application of the rules of procedure by the employees and to make sure the systems are functioning and efficient in practice;
- sanctions control system solutions (screening tools) must be risk-based and proportionate, "smarter", updated and calibrated.

435. The results of the on-site inspections were presented directly to the inspected entities in the inspection reports. Additionally, in order to raise the awareness of the TFS obligations in the financial sector, the EFSA communicated the main results of these inspections to all financial institutions it supervises in the public-private-partnership forum held in October 2021. As a result of the inspections, the EFSA requested 6 entities to provide action plans to eliminate the deficiencies found during the inspections and issued 2 precepts.

436. The EFSA has included specific TFS questions to its off-site questionnaire, including separate TF and PF TFS questions.

437. Analysis of the applied measures did not reveal that, in practice, the shortcoming in sanctioning, as explained in the TC Annex, manifested itself - i.e., that under the misdemeanour proceedings the sanctions set only extend to the violation of a requirement to notify the EFIU of identification of a listed person or entity or submission of false information.

438. Both supervisors suggested to have 2 experienced staff members each, specialised in inspection of implementation of the UN TFS measures. Both staff members of EFSA are trained and underwent the internationally recognised certification on the implementation of the financial sanctions. As also described in (IO.3) the staffing of the EFSA is considered adequate to the population of the supervised entities. The same cannot be said about the EFIU, with more than 10 000 of supervised entities. The EFIU recognised the issue and start taking measures for enhancing its human capacities (see also IO.3).

439. Discussions with the private sectors, especially banks, demonstrated that the conducted inspections had important effect on the sector in terms of their awareness raising, increased attention to the matter and improvement of the respective tools and capacities in this respect.

440. Overall, it can be concluded that over the last year Estonia reinforced its attention towards the implementation of the TFS measures, and demonstrated tangible progress also in supervisory efforts, for which Estonia should be commended.

Overall conclusions on IO.11

441. Estonia has a mechanism for implementation of the UN TFS on PF without delay, but the UN TFS on PF were not communicated to the OEs. Respectively, the OEs were informed about the designations and amendments to those when decisions were made within the EU legislative framework. In practice, while this might have had impact on the timely communication of amendments to the TFS in the DPRK regime, the same did not happen with respect to sanctions on Iran.

442. There were no funds or assets frozen in Estonia pursuant to UN designations related to PF. The authorities suggested that over the period of assessment there were two instances when false positive matches with the UNSCRs on PF were detected. In both instances the entities treated the situation adequately. Among the FIs, banks and other types of institutions that belong to the banking groups demonstrated sufficient understanding of UN TFS requirements, followed by the PSPs, the consumer credit providers, and the exchange services providers. Knowledge, performance and support to the important sectors, such as VASPs, and CSPs are a matter of concern.

443. Over the last year Estonia reinforced its attention towards the implementation of the TFS measures, and demonstrated tangible progress also in supervisory efforts, primarily focusing at the most important sectors, banks and VASPs, for which Estonia should be commended.

444. The country has a developed framework for the counter - proliferation matters within the scope of the SGC. These measures also contribute to prevention of financing of proliferation.

445. **Estonia is rated as having a Substantial level of effectiveness for IO.11.**

5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 4

a) Banks have a good understanding of their ML risks and regularly review their risk assessments. There was evidence of weaker risk understanding and mitigation measures applied in relation to VA services by those banks who also undertake VASP activity. Among non-bank FIs, the understanding of general ML risks is also good, but was of varying quality regarding the sectoral or business specific risks. VASPs, CSPs and other DNFBPs demonstrated a superficial understanding of ML risks to which their individual businesses are exposed. Understanding of TF risk is generally lower across all sectors. Banks, non-bank FIs, VASPs and DNFBPs have a generally good understanding of their AML/CFT obligations, while the awareness of CSPs and real estate agents of their obligations was demonstrated to a lesser degree.

b) There has been a significant investment in AML/CFT compliance and risk management in recent years made by banks, which enhanced the comprehensiveness of their mitigation controls. The mitigating measures applied by non-bank FIs, VASPs and DNFBPs are more general, do not always specifically target the risks, and are limited to the application of generalised due diligence measures supported by some basic monitoring tools. A number of sectors, mostly DNFBPs unduly rely on other parties in the financial system. CSPs also unduly rely on the CDD process undertaken by the state authorities when reviewing e-residency applications.

c) The CDD measures applied by banks in recent years are generally good. Banks carry out their own verifications of the BO information by corroborating data from multiple sources. The level of application of CDD measures by non-bank FIs, VASPs and DNFBPs varies. Some VASPs are using more innovative means to undertake CDD of customers, while others apply more simplistic measures, which are not risk-based. Overall, the concerted effort of the supervisor undertaken in recent years to increase the quality and compliance of the sector is seeing improvements as a result. Among DNFBPs, notaries are implementing more comprehensive CDD measures, including verification of the BO information. On the other hand, the measures of CDD are applied inadequately by the CSP and DPMS sectors.

d) Generally, enhanced measures are applied appropriately by banks. Most banks have a limited appetite for higher risk business which results in concentrating the risks within a small number of banks with higher risk appetite and often less developed specific mitigating measures. Few banks offer correspondent relationships to domestic and foreign high-risk entities. In such cases, the enhanced measures also may include on-site inspections or enhanced

monitoring of transactions through payable through account. VASPs and CSPs are generally less effective in identifying PEPs. Since March 2022, VASPs are required to implement the "travel rule" however it was perceived as problematic to implement by many.

e) For much of the period under review, most of the reporting has been carried out predominantly by banks (70%). Whilst there has been a significant and consistent increase in reporting since 2019 by the VASP sector as a result of the EFIU's outreach program, the number remains lower than expected. The number of reports from notaries has also increased substantially since 2019, while for other DNFBPs, particularly CSPs, the reporting remains alarmingly low.

f) FIs and DNFBPs have generally appropriate control systems in place in the context of the size and materiality of the business, with significant investments made by banks in recent years in AML/CFT compliance and risk management systems. The control systems employed by VASPs and CSPs are overall insufficient.

Recommended Actions

Immediate Outcome 4

a) Estonia should continue to raise awareness of ML risks and AML/CFT obligations, particularly for non-bank FIs and DNFBPs with emphasis on sectorial and business specific risks and to raise TF awareness across all sectors.

b) The EFIU should strengthen its efforts to improve ML and TF risk understanding across VASP and CSP sectors, provide more guidance on TF risk and sector's specific typologies (in particular for VASPs) and ensure that the applied mitigating, CDD and EDD measures are commensurate with their risks. The EFIU should ensure that CSPs undertake independent verifications and do not unduly rely on the checks undertaken by other parties (such as banks and state authorities) when dealing with e-resident customers.

c) The EFIU should take appropriate measures to ensure the implementation of the newly established requirements concerning the VASP sector, particularly regarding the travel rule and internal control requirements and to enhance the control systems employed by VASPs and CSPs.

d) The EFSA should continue to ensure that banks and other FIs are implementing measures commensurate with their risks, especially by those who also undertake VASP activity.

e) The EFSA should continue its efforts to strengthen customer profiling by the FIs, in particular for high-risk customers such as VASPs and CSPs some of whom use generic descriptors in order to bypass enhanced scrutiny.

f) The EFSA should undertake more efforts to enhance the risk understanding and the adequacy of the due diligence measures applied by the investment firms.

g) Supervisory authorities should take necessary actions to ensure that entities are not placing undue reliance on CDD or transaction monitoring carried out by

banks or other parties outside of formal arrangements for CDD reliance or outsourcing.

h) The EFIU should continue to monitor the reporting levels across the sectors and continue outreach activities and sector specific ML/TF trainings, especially for the high-risk sectors where the levels remain lower than expected or are alarmingly low.

446. The relevant IO considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

5.2. Immediate Outcome 4 (Preventive Measures)

447. Considering the materiality and risk in Estonia (see Chapter I, section 1,4,3), the implementation of preventive measures by the relevant sectors is weighted as follows:

- Most important: Banks, VASPs and CSPs;
- Important: Investment firms, Real Estate Agents and Notaries;
- Moderately important: MVTS, Fund managers, DPMSs and Casinos
- Less important: other FIs and DNFBPs including lenders, consumer credit providers, life insurance and the lawyers.

448. As noted in Chapter 1, the banking sector in Estonia is highly concentrated and is the largest single sector by asset size holding about 80% of the total assets of the financial sector. The Estonian banking sector was largely exposed to risks associated with serving non-residents, which has lowered considerably since 2015. In contrast, the highest risk sectors of VASPs and CSPs largely have non-resident clients. There is a clear link between the ML/TF risk posed by these sectors and their large proportion of non-resident customer base. Both sectors grew rapidly over the last 5 years. The number of VASPs has been decreasing since 2020 and the Estonian VASP sector is considered to be concentrated and the growth of the CSP sector was fuelled, in part, by Estonia's e-residency program.

449. The AT's findings on IO.4 are based on interviews with a range of private sector representatives, supervisory findings and enforcement actions, and information from the NRA, as well as other sectoral risk assessments.

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

Banks

450. The interviews of banks showed that they understood their obligations under the MLTFPA and were able to articulate their understanding of those obligations well. Almost all of those interviewed were able to explain that business-wide ML/TF risk assessment was to be undertaken, as well as customer risk assessment following collection of the CDD data; consequently, customers posing a higher risk of ML or TF are subject to additional due diligence measures.

451. The banking sector appeared to have knowledge of the ML risks facing their organisations and demonstrated a good understanding of the rationale behind each of the risk factors they identified. Moreover, the interviewed banks had taken the higher risk factors identified in the NRA and have integrated them into their existing AML/CFT procedures. Such communication to, and acceptance by, the private sector in the relatively short time the current edition of the NRA has been published is a positive indication of the constructive relationship between the EFSA as supervisor and the private sector. However, in relation to the TF risk, those interviewed described a near identical process for screening against financial sanctions and explained what they needed to do in the event of a positive match. Beyond TFS screening, the underlying terrorist financing risks were not well identified or understood by many of those interviewed.

452. During 2014-2015, the EFSA identified serious AML/CFT shortcomings at two banks in relation to high ML/TF risks deriving from non-resident portfolio (which was terminated as a result of the supervisory actions). Since 2016, the banks and other FIs were obliged to submit to the supervisor, via the annual off-site questionnaires, risk assessment and risk appetite documents, thus allowing the EFSA to have a track record of the risk assessments of each supervised entity. Nevertheless, the results of the EFSA's inspections of 2019 revealed shortcomings, including serious, regarding the risk assessment obligation at five banks (including four largest) which represent 90% of the banking sector. In 2020, a positive development in terms of the risk awareness has been observed by the supervisor during the follow-inspections, with only one large bank still having risk-related shortcomings.

453. In addition, in 2020 an information and data-exchange platform was established (AML Bridge) which enables banks and other FIs to cooperate and help raising the awareness of the ML/TF risks and AML/CFT obligations. This private sector' initiative benefited from the support of the EFSA, Data Protection Inspectorate (DPI) and the EFIU and became operational in 2022.

454. All interviewed banks had varying degrees of participation in the NRA process either directly or via the Estonian Banking Association. Three out of five interviewed banks did not participate in the NRA (one of them was not aware of updated AML/CFT offsite returns by the EFSA which included additional questions on the NRA findings). However, the understanding of the NRA demonstrated by banks was generally good with most of them supporting the findings in general terms. In some cases banks identified risks which were either absent from, or were rated lower in the NRA – the FIs who dissented from the NRA findings were able to justify their reasoning well and it was clear that the risks were typically unique to that entity (e.g., the banks views on the risk level of the real estate brokers sector which diverged from the NRA conclusions and the state policy regarding the promotion of e-residency schemes was amongst the heavily criticised national actions).

455. Most of the interviewed banks have a very limited appetite for higher risk businesses, including e-residents, VASPs and CSPs because of the risks posed and due to the previously experienced high-profile scandals by the sector. As a result, many of these businesses are using service providers located outside Estonia. However, this also had a consequence of concentrating higher risk businesses (including foreign) within a small number of banks with higher risk appetite.

456. Banks which demonstrated a higher risk appetite generally had a proportionately increased investment in risk and compliance mitigation resources, the effect of which was evident

during interviews, with a good understanding shown by the board. However, there was evidence that understanding was somewhat weaker in developing areas, such as Fintech, VASPs and similar businesses. The understanding demonstrated was certainly weaker than would be expected from a business servicing those customers. One bank which also undertakes VASP activity demonstrated a much weaker understanding of the risks and the mitigations put in place of VASP activity, often with undue reliance on other parties involved in a transaction. *Non-bank FIs*

457. Most of non-bank FIs demonstrated a good understanding of their AML/CFT obligations. The understanding of ML/TF risks in non-bank FIs is also good, but less robust than for banks and varies among different entities. They had a varying degree of participation in the NRA and not all could confirm their involvement.

458. In some cases, the non-bank FIs dissented from the NRA findings, but were able to justify their reasoning well and it was clear that the risks were typically unique to that entity (e.g., the risk level of the real estate brokers sector and the state policy regarding promotion of e-residency schemes).

459. All non-bank FIs (including the most heavily weighted investment firms' sector) demonstrated varying degrees of understanding the ML risk facing them beyond those risks identified by the NRA. This is generally far less developed than the understanding articulated by the banks and was superficial at times. Although non-banking FIs were able to state various higher risk factors that faced their business (such as non-resident customers, sanctioned individuals and services to VASPs and CSPs), far fewer were able to explain *why* those factors made such customers a higher risk for ML/TF and how those risks applied to their own business and whether those risks were more or less pronounced in the context of their own business model. It should be noted that most non-banking FIs (except for investment firms and small fund managers) similarly had a lower risk appetite meaning that most simply did not on-board or removed customers which posed anything other than a lower risk. Those which did have a higher risk appetite did not generally have the same degree of risk and compliance resourcing, nor the recent investment which the banks have had, and they were generally not able to articulate the same depth of knowledge as their banking counterparts.

460. PSPs typically stated that their risk appetite was minimal and viewed their key risks as VASPs, shell companies and larger transactions (considered to be over €50). The PSP's interviewed appeared to take comfort from the fact that customers' money will be transferred through the banking system at some stage and that the checks undertaken by the banks will reduce the ML/TF risk for the PSP. This reliance is something the AT identified in a number of sectors.

461. The TF risks understanding demonstrated by the non-bank FIs, including the more heavily weighted sectors (investment firms) is also limited. Those interviewed described a near identical process for screening against financial sanctions and explained what they needed to do in the event of a positive match. Beyond TFS screening, those interviewed were unable to articulate the underlying terrorist financing risks.

462. Most non-bank FIs stated that they have an ML/FT risk assessment and most of those interviewed confirmed that they do indeed periodically review their own risk criteria. The risk is categorised based on certain categories prescribed in law or from guidance given by the

authorities (e.g., non-resident customers, VASPs, complex structures and the use of CSPs or strawmen). However, the risk-based approach rarely takes into account risks specific to the sector or institution.

VASPs & CSPs

463. The interviews of VASPs and CSPs showed that they were generally able to articulate their obligations under the MLTFPA well. Almost all of those interviewed were able to explain that identifying customers and the UBO of legal persons was to be undertaken on all customers, and that some form of risk assessment was required of those customers and that those customers posing a higher risk of ML or TF were subject to additional due diligence measures. However, the supervisory information and the sectoral risk assessment indicate that the awareness of the AML/CFT obligations by CSPs is on average low.

464. Both VASPs and CSPs are identified as the two highest risk sectors in Estonia, this was a fact which was broadly agreed with amongst those interviewed by the AT. However, the VASPs and CSPs did not consider that their own respective sectors indeed posed a higher risk, rather both sectors felt that the risk was merely a perception issue and that the authorities just needed to understand their respective industries better. This underestimation of the risks by these sectors could lead to a greater danger of their criminal exploitation. The supervisory findings confirm the shortcomings regarding the risk assessment.

465. VASPs and CSPs demonstrated a superficial understanding of ML risks to which their individual businesses are exposed. Those interviewed stated that they have an ML/FT risk assessment and a number of them confirmed that they do indeed periodically review their own risk criteria. They also referred to the criteria from the MLTFPA such as complex structures and the use nominees and strawmen. VASPs' view was that the predominant risk facing the sector was in respect of the provenance of the virtual asset and so the analysis by those firms was strongly focussed on transaction monitoring rather assessing the wider customer background and profile. CSPs view on risk was very narrow and did not consider risks specific to the CSP sector or to the business itself.

466. Similar to other sectors, VASPs and CSPs demonstrated a limited understanding of the TF risk facing their respective sectors. This was restricted to the elaboration about the risk related to evasion of TF sanctions and geographical risk, i.e. transactions with or customers from higher-risk jurisdictions. No wider consideration of TF risks was demonstrated. Some of the interviewed VASPs expressed the need for more guidance from the supervisor on TF risk and sector's specific TF typologies. This is of particular concern regarding VASPs, as according to the available intelligence, VASPs are being used for TF purposes.

467. The VASPs have a professional association which is supporting the market participants in various sectoral aspects. The AT was informed that a number of VASPs are also part of the data-exchange platform AML Bridge.

DNFBPs

468. Most of the interviewed DNFBPs demonstrated that they understood their obligations under the MLTFPA. Nevertheless, the representatives of the real estate sector, which is material in the Estonian context, demonstrated such awareness to a lesser degree.

469. Most of the DNFBPs the AT interviewed had little to no involvement in the NRA process apart from providing some information in the form of a questionnaire. However almost all were aware of the NRA, some clearly much more recently than others. The understanding demonstrated of the NRA was generally good with most entities agreeing with most of the headline points such as identifying non-resident customers, VASPs and CSPs as posing a higher risk. Although not all DNFBPs were aware of the NRA at the time of publication, a good proportion of the sector were aware of the outreach by the EFIU as supervisor and had attended some sessions.

470. DNFBPs were able to articulate only a superficial understanding of the ML risk environment they operate in. The OEs were able to state various higher risk factors that faced their business (such as non-resident customers, sanctioned individuals and services to VASPs and CSPs), however far fewer were able to explain why those factors made such customers a higher risk for ML/TF and how those risks applied to their own business and whether those risks were more or less pronounced in the context of their own business model. The AT acknowledges that many DNFBPs in Estonia do not target non-resident customers or provide services to higher risk sectors such as VASPs or CSPs. Some sectors such as DPMS and pawnbrokers were not able to articulate even a rudimentary understanding of the ML/TF risks facing Estonia and some were unwilling to even accept that their sector was potentially vulnerable to criminal abuse at all.

471. Most DNFBPs cited criteria from the MLTFPA such as complex structures and the use nominees and strawmen or from guidance given by the authorities like non-resident customers and CSPs and VASPs. However, the risk-based approach almost never took into account risks specific to the sector or business itself.

472. The TF risk was generally not well understood amongst DNFBPs. Those interviewed described a near identical process for screening against financial sanctions and explained what they needed to do in the event of a positive match. Understanding of what to do in the event of false positives was more mixed with a number of DNFBPs having to be guided to the correct answer. Beyond sanctions screening, the underlying terrorist financing risks were poorly identified or understood by many of those interviewed.

5.2.2. Application of risk mitigating measures

473. All obliged entities interviewed demonstrated that they applied mitigation measures, however, the degree of application varies significantly across sectors and is not always risk driven.

Banks and non-bank FIs

474. The EFSA's supervisory projects in recent years has shown that banks have been developing their risk-mitigation activities. As an example, in the years 2020 and 2021, the banking sector significantly increased the number of risk and compliance staff employed (from around 100 to 400 across the sector). The expected result of this investment is to enhance their comprehensive mitigation controls.

475. As noted above, the banking sector demonstrated a more detailed understanding of the rationale behind the risks outlined in the legislation, the NRA and the EFSA's SRA. Control systems focus the mitigation efforts on the specific risks identified, an example given was for customers

of the bank which are PSPs (foreign or domestic) wherein the banks will undertake on-site inspections and assess the PSP's procedures as well as applying additional monitoring and scrutiny to the PSP's customers payments.

476. Whilst FIs generally understood that VASPs and CSPs posed a higher risk and the banking sector particularly were generally able to articulate those risks well, there was evidence that some FIs lacked sufficient technical knowledge to correctly identify customers who were VASPs or CSPs, particularly when those customers described themselves as something more generic (such as an IT company or accountancy/ business consultant respectively). The consequence of this is that some FIs, including some banks, were serving higher risk customers, without applying appropriate mitigation measures to those customers.

477. Non-bank FIs generally viewed the CDD and transaction monitoring requirements mandated by the MLTFPA to be adequate risk mitigation. For higher risk customers controls identified by the AT include undertaking more frequent monitoring of the customer's financial activity and more detailed investigation into the customer's history and background. Whilst it is positive that additional scrutiny takes place for customers identified as posing a higher risk, the measures were very general and rarely took the basis of the underlying risks into account meaning that the mitigation measures are not targeted at the risk identified and so are not applying a risk-based approach in a meaningful way.

478. The heavily weighted investment business sector appeared to have limited controls in place, with those firms exposed to a higher risk environment, articulating little difference in mitigation measures between its higher risk customers regardless of what the actual risk was. Like many non-bank FIs and DNFBPs, there was undue reliance placed on the banks transferring money between the business and the customer. The risk controls in place appear to have been implemented more recently than would be expected, with one firm referring the fact there were lesser requirements in 2017 when in fact the requirements under the MLTFPA remain materially unchanged for investment businesses since well before that time.

479. PSPs similarly viewed the CDD and transaction monitoring requirements mandated by the MLTFPA to be adequate risk mitigation, however this sector also recognised that payable through and segregated accounts represented additional risks unique to their sector. Nevertheless, none of those interviewed offered these services.

480. Many FIs have a low-risk appetite. Certain FIs, which do have a higher risk appetite viewed it as being lower than in reality (bank providing VASP activity and serving high risk businesses and investment firms) and consequently, described weaker mitigation measures applied than expected. The AT also identified a number of cases (PSPs) where customers are viewed as lower risk despite having a number of higher risk indicators, such as PEPs and non-face-to-face business with high volume and values of transactions. This may have an inherent consequence to artificially lower the risk rating of that customer, rather than simply accept the risks and manage them appropriately.

VASPs & CSPs

481. The VASPs interviewed by the assessors recognised that the principal risk facing their business is transactions and the provenance of virtual assets they are handling. Due to this the VASPs informed the AT that they invested in systems to monitor transactions and analysing the

history of the virtual assets that they are handling to determine the likelihood of the virtual asset having been used as the proceeds of crime and, if relevant when. This is, however, not confirmed by the 2021 EFIU sectoral analysis report, which show that the monitoring systems employed by some VASPs have been ineffective.

482. CSPs apply very general due diligence which is not focused on specifically targeting their risk exposure. The EFIU analysis suggests that the risk appetite of CSPs is high with no counterbalance measures for the mitigation of the ML/TF risk that accompanies their activity. In addition, CSPs do not evaluate and apply mitigating measures in relation to the risks accompanying the occasional transactions below the EUR 15 000 threshold (as acknowledged by the NRA).

DNFBPs

483. Most DNFBPs in Estonia are relatively small entities and it was apparent that the risk and compliance resourcing in this sector is more modest than the FIs. DNFBPs generally explained that the CDD and monitoring requirements mandated by the MLTFPA was the extent of the risk mitigation they applied, although many also did high level adverse media screening on a periodic basis. For higher risk customers the entities would obtain additional CDD such as obtaining notarised documents as well as monitoring and reviewing customer's information on a more frequent basis. The measures, however, were simplistic, general and quite prescriptive with little flexibility or appreciation for the underlying cause of the risk.

5.2.3. Application of CDD and record-keeping requirements

Banks and non-bank FIs

484. All FIs were able to articulate the CDD measures which apply to them, with banks providing most comprehensive description. As evidenced by the supervisory findings of the EFSA, the implementation of the CDD obligations by banks and PSPs throughout the period varied.

485. Before 2020, serious AML/CFT shortcomings were identified by the supervisor at four banks, including on the implementation of the CDD and EDD obligations. In two cases, the committed AML/CFT violations are subject to criminal investigations. In 2020, the inspections identified CDD related shortcomings. However, as reported by the supervisors, these deficiencies are less serious.

486. FIs are required to gather from customers which are natural persons basic identification information supported by verification documents; this is typically identification documents which is then verified by the FIs' employees through various databases in Estonia; in addition, FIs screen the clients against publicly available information. When establishing business relationships, information is obtained in the form of either KYC questionnaires or discussions (depending on the nature of the relationship). This information is later used to form a profile of the customer against which their ongoing activities will be monitored. Additional information is commonly sought in higher risk cases (this is both applicable to natural and legal persons).

487. Where a customer is a legal person, FIs generally reported a very similar process. The identification and verification is expanded to include the management board and the beneficial owners of that legal person. Quite a number of FIs reported a few of BO discrepancy data in the Registry (although banks admitted that these cases are rare), as well as unavailability of data in

foreign registries in some circumstances, including due to strawmen and nominee arrangements. However, majority of interviewed FIs are using the Registry not as a single source of verification, but to support the legal documents provided, as evidenced below.

488. All FIs seek to understand the structure of the legal entity by obtaining copies of structure charts and comparing this against publicly available information. In practice very few FIs would consider on-boarding a customer that has a complex ownership (i.e., had more than 2 companies between it and its beneficial owner). Similarly, very few FIs would offer services to legal entities which had any ownership outside of Estonia and beneficial ownership information could not be corroborated directly through Estonian public registries.

489. Estonia has a number of open registers such as the e-business register, which comprises, since 7 March 2022, the Database of Beneficial Owners, and most obliged entities use these registers as part of their CDD and on-boarding process. FIs will generally use the information to corroborate and support evidence of verification that they have independently sought. When asked why the FIs chose not to rely on the data in the registries, most confirmed that the information was not sufficiently reliable, although almost all confirmed that this was typically because the information was out of date rather than through any sort of mal intent by the customer. As such the FIs interviewed would use the data in the registries to support their own verification and, where there is a discrepancy, from March 2022, will request that the customer update the register.

490. Those interviewed were keen to stress that they would have no hesitation to decline business on ML/TF grounds, examples of where business is declined is almost exclusively based on the residence of the customer or its beneficial owner or whether the customer is linked to a VASP. No other examples of circumstances in which a customer would be refused on ML/TF grounds was provided to the AT.

VASPs and CSPs

491. The VASPs and CSPs interviewed have a much greater proportion of non-resident customers than FIs and other DNFBPs. The CSP and VASP sector's customer base is almost exclusively non-resident. All customers (legal and natural) are required to provide identification information at the point of application. Non-resident customers will provide a copy of a passport and (where relevant) an e-residency card. In higher risk cases the CDD information sought is almost universally extended to include proof of address and source of wealth. Where a customer is a legal person, all VASPs and CSPs generally reported a very similar process to the one described for FIs. The interview with VASPs and CSPs showed that they placed significant reliance on the registers and open-source data and often did not seek to independently verify the quality of that data.

492. Interviewed VASPs reported that they typically utilise more innovative means to undertake CDD of customers. In addition to the information sought above, they will seek to authenticate the information through the use of various third-party tools. VASPs understand that their services are more vulnerable to abuse by residents in sanctioned or high-risk jurisdictions. To mitigate this risk a number of VASPs use the geolocation of the customer via their IP address. When the customer logs in the VASP will compare past login data for signs of the use of a VPN which effectively reduces the risk of a customer obscuring their location and utilising the entity's service from a higher risk or sanctioned country.

493. VASPs reported that they focus much more of their mitigation controls on transaction monitoring than most sectors. Transaction monitoring tools are outsourced to third party providers, however, there seems to be less human judgement and consideration of unusual transactions resulting in an overreliance on the tools and systems to identify potential risks to the business. Moreover, the SRA on VASPs indicate generally less effective monitoring systems, which would be in line with the risks of the entities and the results of the supervisory inspections demonstrate that the performance of due diligence measures is among the main identified shortcomings.

494. The CDD measures are applied overall inadequately by the CSPs. This is confirmed by the NRA findings and the results of the supervisory inspections. Whilst most sectors recognised the risks posed by the e-residency program, the CSP sector made significant use of it to help its customers to establish companies, and even obtain licenses within Estonia, mostly in relation companies pre-licensed to undertake VASP activity.

495. The AT identified that CSPs were also placing reliance on the checks that the bank has done leading to a presumption that, if the money is within the financial system, it cannot possibly be proceeds of crime.

496. In addition to placing undue reliance on other parties in the financial system, the AT identified evidence that CSPs in Estonia expected its customers to become e-residents and relied on the CDD process undertaken by the State, this meant that some CSPs did not undertake independent verification of its customers who presented e-residency cards. The AT understands from meetings with the officials involved in reviewing E-Residency applications, throughout the period under review, it did not always do meaningful due diligence to the standards required on e-resident applicants. This gap exposes a material deficiency in a high-risk industry within Estonia's DNFBP sector.

DNFBPs

497. The interviewed DNFBPs reported a similar CDD process as described for FIs. In contrast, a number of DNFBPs placed significant reliance on the registers and open-source data and often did not seek to independently verify the quality of that data. When challenged about the lack of use of independent sources for verification, many of the DNFBPs erroneously believed that the data in open registers was itself subject to some sort of verification and so would be reliable.

498. The AT identified some DNFBPs who placed reliance on other actors within the financial system. In particular, the real estate agents will often place undue reliance on other parties in the transaction such as banks and notaries. The supervisory findings confirm the CDD related shortcomings in the real estate sector.

499. The majority of DNFBPs considered e-residents to be higher risk and would almost universally look through e-residency to identify the customer's true residence and assess any risks arising from that. Almost all DNFBPs took little account of whether a person was an e-resident or not, deeming it an ultimately irrelevant factor.

500. Exemptions are available under the MLTFPA for small transactions which are consistent with the FATF recommendations, however these are typically only used by small businesses for small transactions. It was noted in the NRA that notaries will only look to identify a beneficial owner of a legal entity (including looking through bearer shares) if the transaction is over EUR

15 000 or if there is suspicious activity. However, from interviews with the sector and the CN, the notaries presented diverging views and explained that they would look through the legal structure to the beneficial owner in *all* cases and provided a number of examples in evidence. The AT was also provided with several examples by the interviewed notaries where they updated the BO information of the Registry.

Record keeping (all sectors)

501. Record keeping appears to be consistent across all entities interviewed. All obliged entities agreed that records of transactions must be retained for 5 years from the date that the transaction took place or from the end of the business relationship in line with the retention periods prescribed by law. A handful of banks interviewed explained that they held some records for longer providing justification for doing so, however even in these cases it was not over 7 years. Nevertheless, the supervisory data of both the EFSA and the EFIU show that such deficiencies are still present. This is particularly true for the DNBP sector, where the failure to implement the record keeping requirement is commonly identified.

5.2.4. Application of EDD measures

502. Application of EDD measures are applied to varying degrees by different types of OEs, the banks being the strongest in the application of those measures. Typically, the scope of EDD measures is weaker in other most material sectors, such as VASPs, CSPs and investment firms; and at times underdeveloped in other DNFBP sectors.

Banks and non-bank FIs

503. At the time of the on-site banks appear to have good mitigation measures for higher risk customers as well as comprehensive screening systems which have proven effective. However, this was not always the case for the period under review, as described under CI. 4.3.

PEP

504. In most FIs, the obligation to identify PEPs is well understood and compiled with. Different sources of information are used to identify if a customer is a PEP such as screening with IT-systems, checks from public sources including Estonian registers and declarations from the client.

505. Domestic PEPs are generally well identified and make up almost all of the PEPs served by Estonian FIs. Foreign PEPs are comparatively rare and tend to only be served by a small number of firms which have the risk appetite to serve that sector. This is commensurate with the wider case that few FIs in Estonia have now an appetite for any non-resident customers.

506. Most FIs were able to explain why PEPs are considered to be a higher risk and to articulate the link between a PEP's wealth, funds and the potential corruption risk. This meant that the additional measures required to mitigate those risks were generally better targeted and so more effective. As with risk more broadly, the procedures for PEP identification are more comprehensive amongst the banking sector whilst non-banking FIs, including the heavier weighted investment and PSP sectors, applied more simplistic processes.

507. However, beyond identification and verification, the EDD measures applied by different sectors regarding PEPs are of varying quality: whilst banks reported undertaking EDD measures which include establishing the customer's source of wealth as well as undertaking more detailed

or enhanced ongoing monitoring; other high risk and material sectors such as investment firms, as well, as other non-bank FIs, were not able to articulate concrete EDD measures.

New Technologies

508. The MLTFPA requires obliged entities to manage and assess the risks associated with the introduction and use of new and existing products, business practices or technologies. Although the MLTFPA does not explicitly require that such assessments have to be undertaken *prior* to the launch of new technologies/ services (see R.15.2), it is done in practice.

509. The AT came across an example of a bank which decided to launch a new product – trading in virtual assets and which carried out detailed risk assessment before launching the product (pursuant to the documents provided to the AT), and meetings with the supervisor on the new business model. However, during the interview, there appeared to be a general lack of acknowledgement by the entity (and the supervisor) that the new services are VASP activity and were rather seen as intermediation services (between bank's clients and a VASP).

510. Banks and larger non-bank FIs explained a generally similar, albeit scaled down process – always requiring the compliance officer to review and sign off the systems for AML/CFT compliance before launch. The processes around new or developing technologies, systems development appeared to be substantial and seemingly robust control framework among those larger FIs interviewed by the AT. Smaller FIs' systems were much less complex and there were few examples of circumstances where the requirements around new technologies might be demonstrated.

511. In 2021, the EFSA opened an innovation Hub and issued supervisory policy and guidelines in order to support innovation in the financial sector.

Correspondent banking

512. In general, correspondent banking is not a significant element of most Estonian banks' business. However, three institutions have a large number of correspondent relationships with both Estonian, but mostly with foreign FIs (banks, PSPs and EMIs, investment firms) and high-risk businesses, such VASPs and crowdfunding platforms. As described under R.13, the due diligence process for institutions within the EEA is applied only on a risk-basis. The EFSA's inspection results show that some banks apply EDD by conducting on-site and off-site inspections, as well as KYC checks in respondent FIs. The AT was also provided with examples of applied controls, which included enhanced monitoring of transactions going through the payable through account, random spot checking of CDD of customers of transactions and on-site inspections of the FI to review and assess its internal procedures.

513. Estonian financial sector risks are often connected to the VASPs or MVTS, but also investment firms, through correspondent banking relationships, which is also mentioned by the supervisor as a rising trend (according to the NRA and EFSA SRA findings).

514. Since 2019, there has been a significant increase in the number of criminal threats associated with investment fraud. Most of the suspicious fraud reports received by the EFIU are from a bank that is a correspondent institution for several large Fintech platforms.

Wire Transfers

515. The banks have advised the AT that they use software systems that will block the execution of wire transfers if all required information is not complete or if there are hits with sanction-related lists embedded within the software. This software applies to payments made directly and payments made through payable through accounts or similar.

516. The EFSA has not identified any breaches regarding the wire transfer rules. According to the sample testing made during inspections, the FIs have in place systems and technology which comply with the legislative requirements.

TFS

517. FIs use commercial electronic databases integrated in their information systems, therefore, controls are carried out on the establishment of the customer relationship and later during the customer relationship on a regular basis. All institutions interviewed explained that they also screen their customers, including beneficial owners against UN and other sanctions lists through automated systems that are also based on commercial providers and update several times per day. Nevertheless, the extensive TFS related inspections of the banking sector, covering more than 90% of sector, carried out by the EFSA in 2021 (based on its new powers transferred from the EFIU) show that most banks still do have certain deficiencies. Most of the interviewed banks had positive feedback regarding the EFSA thematic inspections and explained that they improved their automated systems pursuant to the remediation plans or sanctions imposed by the supervisor.

Higher-risk countries

518. FIs consistently demonstrated a good understanding of countries designated a higher risk by the FATF. This is facilitated by the EFSA by sending letters of notifications regarding any changes in the lists of countries designated a higher risk by the FATF, where the EFSA also encourages the FIs under its supervision to take appropriate countermeasures. FIs explained that customers who are from a higher risk jurisdiction are almost universally refused service or have existing business relationships terminated. All those interviewed demonstrated an awareness of the FATF higher risk lists and would have a low-risk appetite for such jurisdictions. All FIs reported that enhanced measures are typically applied to clients from high-risk countries.

VASPs & CSPs

519. VASPs and CSPs were generally able to show that EDD measures should be undertaken when customers were identified as posing a higher risk. As explained above, these sectors deal almost exclusively with non-residents, which implies frequent application of enhanced measures.

520. Most of the interviewed VASPs have described well PEP-related procedures (except one entity) and some reported not accepting PEPs as clients; those that are accepting clients, outsource PEP related checks to the third-party providers. However, the supervisory data shows that there were numerous occasions where VASPs were found not identifying PEPs correctly; this might be partly attributed to the less effective surveillance and monitoring systems for the majority of VASPs.[167]

[167] Sectoral Risk Assessment of VASPs (January 2022), page 5, 25

521. Since March 2022 VASPs are required to comply with wire transfer rules (*travel rule*). This is a positive technical development for which the Estonian authorities are commended. However, most of the interviewed VASPs expressed the view that the new requirements would be extremely difficult to implement effectively and a commitment by all the market participants would be essential.

522. For the implementation of TFS obligations, VASPs rely on commercial electronic databases which plug into their internal databases and works in a similar fashion to FIs. The systems will automatically screen customers during on-boarding, prior to transactions and otherwise at least once per day. However, the EFIU analysis shows that third party service providers that are used for screening are not reliable in all cases and thus OEs are expected to adopt additional mitigating measures.

523. CSPs do not invest in risk management technology solutions and only small part of the sector is considered (based on the EFIU analysis) to have sufficient available sources in order to identify PEPs.[168] The identification and verification of PEPs is usually carried out based on questionnaires (client's declaration) or information from open public sources. Considering the risks of the sector deriving from serving mostly non-resident customers, these measures appear to be insufficient.

524. VASPs and CSPs generally demonstrated a good awareness of the FATF higher risk jurisdictions. However, even after identifying such jurisdictions, their approach to engaging in business relationship with such clients is relatively soft and insufficient attention is put to mitigation.

DNFPBs

525. DNFBPs are generally aware of the PEP-related obligations and are predominantly serving domestic PEPs, which is in line with their risk profile. All DNFBP sectors commonly describe EDD measures, such as source of wealth/funds, enhanced monitoring, management acceptance. The findings described in relation to the application of CDD measures by the DNFBP sector are applicable here.

526. Outside of the FI and VASP sector the new technology risk assessment framework is less comprehensive, however it must be noted that the introduction of new technologies and innovation amongst DNFBPs generally was much less widespread.

527. Many DNFBPs interviewed explained that they screen their customers, including beneficial owners against UN sanctions lists; however, this is not the always the case in the DPMS, casinos, pawnshops, legal and accountancy sectors. Smaller DNFBPs, including sectors of relative importance, such as DPMSs and casinos, were often reliant on manual processes – screening customers when on boarding and routinely screening their client base once per quarter or annually from the lists published on the EFIU's website, allowing for a considerable period of time to elapse following changes to the lists before potentially sanctioned customers are identified.

528. Many DNFBPs struggled to articulate a meaningful understanding of why jurisdictions pose a higher risk for ML or TF (some even struggling to identify locations which pose a greater TF risk than an ML risk). The AT believe that some DNFBPs only identified jurisdictions as posing a higher

[168] NRA 2020, Chapter 11, page 7.

risk merely because they were instructed to do so by published guidance or relevant supervisors without any understanding as to why.

5.2.5. Reporting obligations and tipping off

529. . OEs are required to submit five types of suspicion-based reports: suspicious transaction reports (STRs), terrorism financing reports (TFRs), unusual transaction reports (UTRs), unusual activity reports (UARs), unusual activity reports relating to terrorism financing (TF_UARs). Additionally, the reporting obligation includes the international sanctions reports (ISRs) and cash transaction reports (CTRs). The reporting obligation is fulfilled through a dedicated web portal.

530. All OEs are aware of their reporting obligations and are provided with guidance by the EFIU, which explains relevant criteria for categorisation of reports. All those interviewed were able to articulate their understanding of which report should be filed in what circumstances with confidence. Nevertheless, their understanding and interpretation of which type of report shall be filed varied. This might be impacted by the quality of the provided guidance (which is analysed under IO.6).

531. On the whole, FIs have demonstrated a stronger and more consistent track record over the period under review than DNFBPs which, although improving slowly, continue to have very low levels of reporting. Since 2019, the number of the annually filed reports has increased substantially (4600 reports in 2019, 6300 reports - 2020 and 14500 in 2021). 2019 and 2020 show a 50% increase. The increase follows the outreach and supervisory activities with a number of sectors, mostly material sectors, such as VASPs, notaries and real estate agents (although the number of reports filed by the latter remains very low).

532. The EFIU also explained that they have increased the outreach across all obliged entities in order to improve the level and quality of reporting. These activities were carried out at the same time as the significant investment in the EFIU's systems. The interviewed OEs confirmed that they noticed an increase of the training and outreach activities since 2019.

533. Since 20220, the EFIU provides annual sectoral feedback[169] and thorough the period under review – operational (individual feedback), which were generally appreciated by the private sector. The OEs receive operational feedback when additional information is needed by the EFIU, the provided data is not sufficient or contains some errors. This was confirmed to the AT by a small number of those interviewed who had received such feedback. Those interviewed satisfied the assessment team that restrictions around tipping off are generally well understood and complied with.

534. The table below outlines the number of reports submitted by the OEs over the period under review.

Table N°5.1: Number of reports (except CTRs) submitted by OEs to the FIU

OEs	2016		2017		2018		2019		2020		2021	
	No	%	No	%	No	%	No	%	No	%	No	%
FIs												
Banks	2065	65,89%	2306	70,37%	2152	68,93%	2902	62,91%	4586	72,62%	11072	76,54%

[169] https://www.fiu.ee/en/annual-reports-and-surveys-estonian-fiu/feedback-fiu

PSPs	67	2,14%	70	2,14%	157	5,03%	53	1,15%	35	0,55%	465	3,21%
Money Remittance	642	20,49%	521	15,9%	326	10,44%	526	11,40%	438	6,94%	469	3,24%
Investment firms	14	0,45%	11	0,34%	11	0,35%	32	0,69%	35	0,55%	10	0,07%
Insurance sector	0	0	1	0,03%	2	0,06%	2	0,04%	0	0	0	0
Consumer Credit	8	0,26%	25	0,76%	31	0,99%	35	0,76%	43	0,68%	47	0,32%
Currency exchange	149	4,75%	161	4,91%	35	1,12%	36	0,78%	59	0,93%	37	0,26%
Other FIs	1	0,03%	0	0	0	0	0	0	1	0,02%	11	0,08%
VASPs												
VASPs	1	0,03%	3	0,09%	8	0,26%	399	8,65%	528	8,36%	1852	12,80%
DNFBPs												
CSPs	0	0	2	0,06%	0	0	7	0,15%	11	0,17%	6	0,04%
Real estate agents	0	0	0	0	0	0	4	0,09%	7	0,11%	5	0,03%
DPMS/ traders	2	0,06%	2	0,06%	7	0,22%	10	0,22%	16	0,25%	31	0,21%
Casinos/ gambling	62	1,98%	39	1,19%	58	1,86%	91	1,97%	40	0,63%	57	0,39%
Notaries	33	1,05%	36	1,10%	61	1,95%	271	5,87%	119	1,88%	114	0,79%
Lawyers/other legal prof.	16	0,51%	15	0,46%	13	0,42%	21	0,46%	8	0,13%	19	0,13%
Accountants			1	0,03%	7	0,22%	10	0,22%	9	0,14%	9	0,06%
Auditors	1	0,03%	1	0,03%	5	0,16%	13	0,28%	9	0,14%	11	0,08%
Other (non-OEs)	73	2,32%	83	2,53%	249	7,97%	201	4,35 %	371	5,87 %	250	1,72%
TOTAL	3134	100%	3277	100 %	3122	100%	4613	100%	6315	100%	14465	100%

535. Overall, most of reports come from the banking sector, which files around 70% of reports, followed by MVTS providers (mostly money remittance) at around 10% of reports and VASPs with about 8-12% of the total filed reports (for the period 2019-2021). The remaining 19 sectors together account for only 12% of reports.

536. The share of reports submitted by banks is reflective of the risk and materiality of the sector. Nevertheless, the AT also identified a significant number of retrospective reports in relation to three banks involved in high profile ML cases, which indicates that their systems lacked proactive and timely identification of red flags. As a result of the supervisory efforts (including a prohibition to operate and a dissuasive fine), major banks have significantly increased their investments in IT development and improvement of audit. In 2020, the EFSA identified shortcomings regarding monitoring tools and reporting obligations at important banks. However, those were not considered to be serious and were remedied by the entities (as result of a precept). In 2021 around 62% of the reports filed by the banking sector, were submitted by one bank and were related to investment fraud. Overall, this is consistent with the main ML threat of the country – investment frauds which are continually increasing since 2019, but also with the risk of the entity, which is a correspondent institution for several large Fintech platforms.

537. The increased cybercrime (especially during the COVID-19 period) is also considered by the authorities to be the main reason for the significantly higher number of reports submitted by PSPs in 2021 compared to 2020 (456 in 2021 and 35 in 2020).

538. The VASP sector represent around 8 to 12% of the reports made over the last three years. The EFIU data analysis of 2021 shows that in 2020 – 2021 (eight months), only 28% of the VASPs that were actively providing services (defined as having a turnover of over EUR 2 000) had made reports to the EFIU. By the end of 2021, the reporting level, due to the training, feedback and supervisory activities of the EFIU, had risen to around 40%. However, considering the size and materiality of the sector, which is associated with the highest ML/TF risk, the number of reports remains lower than expected. This is confirmed by the 2021 EFIU sectoral feedback, which

concludes that although the reporting activity of VASPs shows signs of improvement, the receipt of only few reports from entities with the highest turnover is a sign of risk.

539. The reporting amongst the CSP sector is alarmingly low. 11 reports made in a year (2021) indicate approximately that an average of 1 report is filed for every 30 CSPs licensed. The CSP sector demonstrated a very poor understanding of the risks facing it and where risks were identified to them, either by published documents such as the NRA, or by the AT in interviews, the materiality of those risks was largely played down by the CSPs.

540. Following outreach of the EFIU in 2019, the number of reports from the notary sector have increased from 36 to 114 in a year – in a sector with only 88 members this shows a good improvement. The filed reports also reflect the risks associated with the sector, in particular real estate transactions, including one involving virtual assets.

541. Real estate agents have only begun reporting in 2019, following the EFIU outreach and the number of the filed reports is low considering the materiality of the sector. When interviewed, only a few firms appeared to be aware of the training made available by the EFIU. Although all were aware of the published guidance, for some this seemed to be very recent news. When discussing with the sector, it became apparent that they will often place undue reliance on other parties in the transaction such as banks and notaries, assuming that they would identify if suspicious activity is taking place and they (the bank or notary) would take action and make the appropriate report.

5.2.6. Internal controls and legal/regulatory requirements impending implementation

Banks and non-bank FIs

542. Banks demonstrated a positive AML/CFT compliance culture and described appropriate control systems in place which were adapted to their size and risks. The banking sector have invested heavily in compliance and risk systems and personnel from 2018 onwards. The number of compliance and risk personnel in the banking sector increased from 32 in 2017 to 431 in 2021. This is due to multiple factors including the efforts made by the EFSA, more dissuasive sanctions imposed on the banks over that period and, better education and understanding by the banking sector of the importance of preventing ML and TF in the context of the high-profile ML cases which affected the country.

543. 68% of banks operating in Estonia are owned Nordic financial groups. These banks have adopted the internal control systems of their respective groups, varying those control frameworks only where there are Estonian specific requirements. The EFSA's onsite examinations' findings up to 2020 show commonly the shortcomings related to internal controls, also involving well publicised banks' failures and the lack of management's involvement in AML/CFT and risk management. The AT identified some isolated instances where a Group internal audit had identified internal control or governance deficiencies within the Estonian part of the business, however this was not reported to the local management board for some time afterwards (years in some cases) and so the deficiencies were not rectified in a timely manner.

544. Larger FIs described appropriate control systems in place which included an internal audit function, whereas in the smaller FIs this function was outsourced to an external firm. Amongst

very small FIs internal audit is undertaken by the compliance officer which may create a conflict of interest if not properly managed. The majority of FIs spoken to appear to the AT to enjoy support from their senior management and were adequately resourced – particularly amongst those FIs interviewed.

545. The EFSA conducts an annual review of firms internal control systems as part of the annual off-site questionnaire. The EFSA's findings show that internal control activities are coherent with the size, complexity and type of business of the FIs under its supervision and that there is a general improvement of the quality of their internal control systems.

VASP

546. According to the EFIU analysis, VASPs, including those with a high turnover, have predominantly 1-2 employees. This indicates that the business system of the majority of market participants do not consider expenses of the monitoring systems or the necessary staff, or they are outsourcing these activities. A high number of VASPs have appointed the same person as a contact point for AML/CFT purposes. The supervisory inspections identified a number of shortcomings in the rules of procedure, as well as in the risk assessments. The EFIU has undertaken a series of efforts in order to improve the quality of the market participants, including the revision of the licensing process and license revocations. Some of the interviewed VASPs and the representatives of the VASP association expressed a positive opinion about the reform.

DNFBPs

547. The internal control systems described by DNFBPs were generally appropriate in context of the size and materiality of the business. CSPs, weighted as the most important DNFBP sector, described generally a similar structure to the wider DNFBP sector, however the results of the NRA indicate an overall insufficient compliance control systems employed by CSPs and that approximately 75% of the providers do not invest in risk management technology solutions.

548. Most DNFBPs were critical regarding the significant lack of guidance for setting up their internal control's framework for AML/CFT implementation (e.g., procedures) and some reported having relied on the guidance published by other countries (e.g., some casinos reported using Maltese guidance). In 2019, the EFIU prepared sample guidelines (rules of procedure and internal control rules) for the real estate agents and in April 2020 published AML/CFT guidelines which tackle the organisational structure and the rules of procedures for the supervised entities. All DNFBPs (and several VASPs) expressed the need for more comprehensive guidance on TF identification, including typologies.

549. The MLTFPA does not require DNFBPs to have an internal audit function however despite this technical deficiency, in practice most mid-sized and larger DNFBPs do appoint some form of internal audit function whereas the majority of smaller firms do not appear to have such a function.

All

550. All businesses interviewed by the AT had appointed an individual who is responsible for the AML/CFT compliance of the entity. Newly appointed staff members are subject to vetting prior to their appointment, the scope of the vetting varies significantly across the FI sectors and appears largely proportionate to the size of the obliged entity. Generally, vetting will include a review of an applicant's employment history and qualifications as well as a review of open-source

materials such as adverse media, the population register, court records and criminal records within Estonia. These screening procedures appear to be sufficient to ensure a high standard when hiring employees, it should be noted that most banks interviewed do go beyond these processes.

551. All interviewed explained that they arranged AML/CFT training for their staff shortly after they started employment and annually on an ongoing basis. The training provided and delivery methods varied across entities interviewed but typically included online training and some form of mentoring for larger FIs, with smaller entities employing more direct oversight and training from the compliance officer or more experienced staff.

552. All those that discussed training with the AT highlighted that the training would include information on the staff member's AML/CFT obligations and relevant changes, updates to that legal framework as well as sanctions and how sanctions screening works practically for that business. Those obliged entities which are part of a Group, aligned their training regime and curriculum to that of the parent varying when appropriate for Estonia.

553. Estonia has a relatively small population and so the pool of risk and compliance expertise is smaller than many other jurisdictions. The significant investment made by the banking sector since 2018 in compliance and risk systems and personnel has had an unintended consequence of causing the number of risk and compliance staff to reduce in all other sectors creating resource pressures elsewhere in the financial, DNFBP and VASP sector.

Overall conclusions on IO.4

554. Banking sector, which is weighted as one of the most important sectors, have a good level of understanding of their ML risks. Preventive measures in the banking sector are steadily improving since 2020 and there was a significant investment in AML/CFT compliance and risk management which enhanced the comprehensiveness of their mitigation controls. Most of reports come from the banking sector (70%). Throughout the period under review, this was not the case and four banks have committed serious AML/CFT violations. Since 2020, due to the supervisory measures a positive development is noted. This impacted the risk appetite of most banks which is limited for higher risk business. However, it is also observed a concentration of the risks within a small number of banks with higher risk appetite, mostly in relation to correspondent relationships with foreign high-risk business (VASPs, PSPs, EMIs and Fintech platforms) and VASP activity. One bank which also undertake VASP activity demonstrated a much weaker understanding of the risks and the mitigations put in place of VASP activity.

555. VASPs (weighted as one of the most important sectors) generally, throughout the period under review, demonstrated a rather superficial understanding of risks and general mitigating measures applied. The preventive measures are often not applied in accordance with the specific business risk. At the same time, the reinforced supervisory attention towards the quality and compliance of the sector since 2020 indicate some positive results. VASPs had to adjust their business to higher licensing standards, including IT tools. Since 2019, as a result of the outreach activities the number of filed reports increased considerably, although a higher number is expected.

556. CSPs, also weighted as one of the most important sectors, demonstrated insufficient risk understanding and less effective preventive measures. The level of reporting by the sector is also alarmingly low.

557. The understanding of ML risks and the effectiveness of preventive measures is varied across the sectors. More weight is given to the shortcomings identified in the most important sectors. The AT believes that IO.4 is achieved to some extent and major improvements are needed.

558. **Estonia is rated as having a Moderate level of effectiveness for IO.4.**

6. SUPERVISION

6.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 3

a) Both main supervisors – the EFSA and the EFIU have revised their supervisory approach and increased their capacity since 2019 in order to address the emerging risks posed by the supervised sectors.

b) The licensing process for FIs includes comprehensive fitness and propriety checks in order to ensure criminals and their associates are not beneficial owners or hold controlling interests in FIs. Robust checks are also in place to ensure persons holding key functions are fit and proper. Individuals are reassessed however there are cases of such checks being delayed or avoided.

c) Until 2020, the licensing process for VASPs lacked robustness, resulting in a large number of entities being licensed without having adequate systems and procedures or a connection to Estonia, and being largely misused for criminal purposes. Since 2020 the EFIU has made considerable efforts to improve the licensing of the VASP sector and to removing the licences of many of the unfit entities and increasing the EFIU's capacity. In March 2022 the framework for licensing VASPs was further strengthened. The fit and propriety checks carried out by the EFIU rarely involve contacting relevant foreign authorities, which is particularly important for the VASP, but also for the CSP sectors, considering the significant proportion of their foreign connection.

d) The existing supervisory arrangements between the EFSA and the EFIU regarding the entities which are carrying out both financial and VA related services are impacted by some uncertainties around the identification of the VA activity in an FI, identification of an FI activity carried out by a VASP and the designated supervisor for the VASPs which obtained subsequently an FI licence.

e) There are varying standards in the approaches taken to licensing across the various DNFBP sectors. Not all DNFBP sectors are subject to licensing or fit and proper assessment before being permitted to operate.

f) Sanctions for carrying on a regulated activity without an appropriate licence or authorisation are ineffective. The number of convictions for illegal economic activity compared to the number of referrals made by the supervisors is extremely low. For the current mechanism to be effective, supervisors would require additional powers.

g) The risk analysis tools employed by the EFSA are comprehensive and draw from multiple qualitative and quantitative sources. However, the assessment of the ML/TF risks is often being applied too narrowly, or certain risks are given undue weight at the expense of other factors. This resulted in a detrimental impact on the effectiveness of a risk based supervisory methodology.

h) Both of Estonia's most risky and material sectors (VASPs and CSPs) fall under the supervision of the EFIU and whilst it is clear that the authority is now developing a better understanding of the risks of these sectors and the resources have only very recently been increased for the EFIU as a whole, the supervisory activity was not carried out on a risk-sensitive basis for the most period under review. Supervision by the SRBs considers some risks specific for the sectors, however it cannot be considered as truly being carried out on a risk-sensitive basis.

i) Overall, the supervisors rely heavily on remedial supervisory measures to deal with breaches and there are cases which would require more prompt supervisory actions. The effectiveness of the available sanctioning tools for imposing fines for breaches of the AML/CFT obligations is significantly affected by the limitations of the applicable misdemeanour proceedings, such as the level of those fines and procedural constraints.

j) The relationship between the supervisors and the obliged entities is generally positive. In particular, the open and proactive communication by the EFSA was highlighted.

Recommended Actions

Immediate Outcome 3

a) The authorities should ensure that all FI's DNFBP's and VASPs are subject to an appropriate and robust licencing or authorisation process, including by carrying out the periodic suitability re-assessment process in a timely manner (EFSA), by effectively applying the newly introduced (in March 2022) licensing requirements for VASPs and that the fit and propriety checks consider the information available to foreign authorities, especially for the sectors with a significant foreign connection such as VASPs and CSPs (EFIU).

b) The EFIU and the EFSA should proactively assess whether VASPs may be undertaking other regulated activities such as services to securities, payment services, electronic money issuance or VASP lending, or whether FIs may be undertaking VASP activity, and ensure they are appropriately licensed and supervised. The existing supervisory arrangements shall be clarified.

c) The supervisory authorities should continue their efforts to identify and prevent unlicensed activity and be given appropriate powers to punish those acting without a licence or authorisation.

d) The supervisors should undertake a comprehensive review of their risk-based approach to ensure that there is increased and proportionate focus on higher risk sectors and that there is appropriate focus on all higher risk matters.

e) The EFSA should undertake a comprehensive review of those entities it rates as "very low risk" and of the criteria in the EFSA's procedures for determining the very low risk level. The degree of scrutiny and supervision of the re-rated entities should be revised accordingly.

f) The EFIU should develop and implement a system for liaising with foreign authorities to ascertain whether they have information relevant for assessing and re-assessing the fit and properness of applicants or key function holders.

g) The supervisors should be given appropriate sanctioning powers in order to impose financial penalties where OEs are found to be deficient to ensure that sanctions are effective, proportionate and dissuasive.

h) The CN should undertake, and the BA should enhance its program of risk based on site inspections of its members. The inspections process should be thorough and robust similar to that undertaken by other Estonian supervisors.

559. The relevant IO considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

6.2. Immediate Outcome 3 (Supervision)

560. There are two main AML/CFT supervisory authorities in Estonia – the EFSA and the EFIU. The EFSA is responsible for the supervision of the vast majority of the FIs and the EFIU for the DNFBPs (except lawyers and notaries). The EFIU also supervises VASPs and certain less material FIs, including currency exchange offices. The AML/CFT oversight of lawyers and notaries is carried out by the BA and CN respectively. The competence for the licencing process of FIs and DNFBPs is split across 5 bodies. The EFSA licences most Estonian FIs and the EFIU licenses most DNFBPs, VASPs and those FIs not overseen by the EFSA. The ETCB licenses casinos and the OBA is responsible for auditors' licensing. The BA is responsible for the licencing of lawyers and the MoJ is the licencing authority for notaries. Real estate agents, accountants and tax consultants are not required to be licensed or authorised and, therefore, are not subject to fitness and propriety assessment by any authority. The breakdown of the licensing and supervisory arrangements is described under Chapter 1 of the report, p.1.4.6.

561. The weighting given to Estonian OEs regarding supervision, based on the relative importance of each sector, is the same as detailed under Chapter 1, p.1.4.3 and applied for preventive measures (IO.4).

6.2.1. Licensing, registration and controls preventing criminals and associates from entering the market

EFSA

562. The general process for licensing of new entities requires the submission of relevant documentation from the applicant, including the completed extensive fit and proper questionnaire. This documentation is reviewed by a working group formed within the EFSA which is comprised of personnel from all departments, including the relevant supervisory team (such as banking, investments, etc.), the fit and proper assessment team, the AML/CFT team, business conduct team, prudential team, and the risk analysis team. The working group assesses the applicant's internal control processes, capital requirements, sources of funds, risk management procedures and the fitness and propriety of individuals holding a senior

management role. Formally, the licencing process may take up to 12 months in relation to banks, ultimately licensed by the European Central Bank (ECB), in close cooperation with the EFSA, and 6 months for other FIs. In practice, the process may take longer which leaves room for more thorough checks. The AT was informed by the private sector on several occasions of informal consultations with the EFSA on the feasibility of the business plan and other licencing requirements, before a formal application.

563. The EFSA issued specific Guidelines which provides to the market additional explanations and specifies the main expectations regarding the fit and proper assessment. Fit and proper assessments are undertaken on the owners, beneficial owners, all members of the supervisory board and management board, and individuals holding significant or controlling interests. A person will be considered not fit and proper (and so not permitted to take up the role) if they have been accused, suspected of, convicted of, or otherwise involved in a criminal offence, or if they do not meet the impeccable business reputation requirement. This information is verified against a number of sources, including the Estonian criminal records register, records held by the Courts, the business and beneficial ownership registry, data provided by external commercial databased and open sources. The EFSA will also proactively contact the EFIU, ETCB, Police and Border Guard Agency, the Consumer Protection Agency and other competent authorities. In cases where the applicant is a foreign citizen or has a connection with a foreign country, the EFSA will contact the relevant foreign regulators for any information about the applicant or any individuals associated to that applicant.

564. As part of the assessment process, the EFSA will contact the applicant and explain whether it is minded to refuse the issuance of a licence. In the majority of such cases, the application will be withdrawn in order to avoid a negative decision. When the applicant is not withdrawing the application, the EFSA will take the decision to refuse it. The power to refuse an application sits with the management board of the EFSA, with the exception of banks which rests with the ECB.

Table N°6.1: EFSA licensing statistics

	2015	2016	2017	2018	2019	2020	2021
Licence applications	61	34	14	13	10	27	26
Withdrawals before formal decision	14	13	5	7	3	13	3
Total refusals	1	1	1	2	1	6	6
% non-issuance of a licence	24.6%	41%	43%	69%	40%	70.3%	34.6%
Incl. refusals with a fit and proper element	1	1	1	1	0	3	1
% refusals with a fit and proper element	100%	100%	100%	50%	0%	50%	16.7%

565. As can be observed from the table above, there is an increasing rate of refusal decisions. Together with the number of withdrawal cases before a formal decision, the rate of *refusals*[170] varies roughly between 30% and 70%. Frequent reasons for refusals or withdrawals are the failure to meet fit and proper requirements by the individuals owning/controlling or managing the applicant. The EFSA has found individuals not fit and proper based on a past accusation of a criminal offence (for which the individual was acquitted), and the Court upheld the EFSA's

[170] Formal refusals and withdrawals before a formal decision

determination of unfitness when the individual appealed the case. Likewise, a great emphasis is placed on the reputation and the appropriate qualifications of the individual. In some cases, the knowledge requirement was essential and helped to identify attempts to promote strawmen. Estonia has a very small talent pool to draw from meaning that private sector firms often struggle to recruit quality candidates which in turn results in a greater proportion of individuals being refused by the EFSA. Other recurrent reasons for refusals include a lack of economic substance or connection to Estonia. This indicates an overall rigorous assessment process implemented by the EFSA for ensuring the quality of the sectors under its competence.

566. A person seeking a *qualifying holding* is required by the legislation to have an *impeccable business reputation* which includes an assessment as to whether the individual has a criminal record, is suspected, or is otherwise involved in a criminal offence, or is associated with a criminal. The EFSA also has the power to refuse the acquisition of a qualifying holding if there is a justified suspicion that the acquisition, possession or increase of the holding or the control over the FI is connected to ML or TF or even if it increases such risks. In the case of banks, the competence to decide on qualifying holdings belongs to the ECB.

Table N°6.2: EFSA's statistics on the proceedings on qualifying holdings

	2015	2016	2017	2018	2019	2020	2021
Qualifying holding (by no of subjects)	63	40	25	27	26	29	28
Qualifying holding (by no of persons)	184	119	83	55	106	88	134
Positive decisions (no&%):							
by subjects	48 (76%)	23 (58%)	18 (72%)	17 (63%)	13 (50%)	15 (52%)	14 (50%)
by persons	149(81%)	87 (73%)	59 (71%)	46 (84%)	51 (48%)	40 (45%)	66 (49%)

567. Like individuals proposed to be appointed to the management and supervisory board of an FI, before making a formal decision to refuse an application for a qualifying holding, the EFSA will explain to the applicant that it is minded to refuse the application, including its reasons, and the subject or individual will usually withdraw their application. The number of subjects applying for a qualifying holding has remained broadly at the same level since 2017, however the number of those approved to take a qualifying holding in an FI has decreased significantly due in large part to the EFSA's increasing rigour around those applicants. Failure to meet the fit and proper requirements, including the *impeccable business reputation* requirement, is among the main reasons for the refusal decisions or the withdrawals as a result of the EFSA's inquiries. Examples cited include: malevolent behaviour in a previous position, which included disregarding the AML/CFT obligations; accusations by the business partners of fraudulent activity; affiliation with a company suspected to be involved in ML; potential involvement in dubious activity, previous convictions (15 years before the EFSA's assessment) for crimes against property and public order (including robberies of a bank's branch), etc. Other reasons refer to the non-transparent price of the transaction through the distortion between the share purchase price and the book value of the share.

568. Fit and proper assessments are part of ongoing supervision as suitability of the manager must be met any moment in time. FIs are required to perform periodic suitability re-assessment at least annually and notify the EFSA of circumstances which may have a negative impact on the relevant person's suitability. The number of such notifications received by the EFSA remains unknown. Additionally, the EFSA has other tools at its disposal, such as the annual thematic offsite

inspections conducted by the legal department of the EFSA. In 2019, 18 FIs and in 2021 – 21 FIs, covering all sectors under supervision, were subjects of such inspections.[171] Likewise, in 2019 and 2020 the EFSA commenced, on its own initiative, two fit and proper re-assessments to reconsider the suitability of two mangers of an OE which were carried out following findings from an inspection of that OE. The assessment outcome was that both managers were suitable.

569. The processes highlighted above supported by the number of negative decisions and the withdrawal notifications appears to indicate an overall robust and effective licensing process aiming at preventing criminals and their associates to be part of the financial market. The EFSA also has in place and applies a periodic suitability re-assessment process. Nevertheless, there are several high-profile ML cases which significantly affected the country's reputation, and which raise questions regarding the suitability of management of those banks and on the effectiveness of the periodic suitability re-assessment process. As described under CI 3.4, there are cases where senior managers were able to avoid the fit and proper re-assessment process and leave their posts before any formal action was taken, including any sanction being applied to them.

570. The EFSA routinely searches social media and other public advertisements for businesses which operate in the regulated sector and are not appropriately licensed. In 2003 the EFSA's consumer website[172] was established to give individuals and businesses the opportunity to disclose cases of unlicensed regulated activity. Moreover, the EFSA has a dedicated space on its website and informs the wider public of such cases, including potential fraud schemes, when identifies them. It does so proactively, despite the lack of a clear legal basis for the publication of the alerts. In some cases, the subjects of the alerts appealed in court the EFSA's decision, which proves the impact of such alerts.

571. The unlicensed economic activity can be punished only criminally. The described above efforts resulted in 57 referrals made by the EFSA to the prosecutor's office, during 2017-2021, most of them being investigated (93%), which indicates a good quality of those reports. Nevertheless, only in 4 cases was a conviction achieved (7%). Moreover, the ratio of the successful convictions could be lower, as the analysis does not consider the number of referrals made by the EFIU (due to their absence). The very low success rate may be explained by the judicial interpretation (including the Supreme Court of Justice) of the legal provisions, which requires that the unlicensed services to be provided to Estonian consumers and limits the ability to achieve a conviction in cases when an Estonian company provides services abroad.

EFIU

572. The Supervisory Department of the EFIU is responsible for assessing the applications of new entities and the assessment of individuals applying for senior roles within certain FIs (which are not licensed by the EFSA), VASPs and most DNFBPs. The power to approve or refuse an application rest with the head of the EFIU.

573. Certain DNFBPs which are supervised by the EFIU, such as real estate agents, accountants and tax consultants do not have licensing or registration obligation and are not subject to assessment for fitness and propriety but have special requirements. A real estate agent,

[171] In 2020, the inspection was postponed due to COVID-19.

[172] www.minuraha.ee

accountant or tax consultant must not allow its owners, beneficial owners, members of its management or supervisory board to have an unexpired conviction for an economic criminal offence or a criminal offence against property, the state or public trust. However, this is not monitored or supervised by any state body.

574. The licensing process, including the fit and proper assessment, is based on the internal EFIU Guidelines and the *fit and proper* questionnaire which has to be completed by the applicant. The same market entry process is applied for the OEs under the EFIU responsibility, with additional more rigorous requirements introduced for VASPs in 2020 (e.g., a single license for all VA related activities; increased minimum of the share capital; the requirement for the management to reside in Estonia) and 2022 (e.g., further increased minimum of the share capital; more information about the business, including financial information, a feasible business plan, information on the technology systems, financial audit).

575. One aspect of the licensing process which required significant improvement was the processing time of the applications. Before 2020, the time limit was 30 working days, which is considered insufficient. It was changed to 60 working days since the date of the application with a possible extension up to 120 days. Although a positive step, in the absence of any positive or negative decision made by the EFIU within this timeframe, the license would be considered as automatically granted (a legal interpretation upheld by several court rulings). This impacted negatively the effectiveness of the licensing process, especially regarding more complex applications, such as those for VASP licenses, and which would require a longer period for processing. Only in 2022, there were about 55 applications related to VASPs which were processed for more than 120 days. The authorities' efforts to remedy this situation are commendable and since March 2022, the processing time is calculated from the date when *all information needed by the supervisor for making a decision is submitted*, thus allowing the EFIU sufficient time for processing the applications and a licence is now automatically deemed refused (rather than granted) should the time limit expire.

576. Fit and proper assessments are undertaken on the owners, beneficial owners and members of the management body. A specific feature of the Estonian system is that the compliance officers of all OEs are also subject to *fit and proper* checks, carried out by the EFIU, aiming at verifying their suitability and reliability. Beside the requirements on the appropriate education, professional suitability and experience, a compliance officer/ candidate must also meet the *impeccable reputation* criteria.

577. A person will be considered not fit and proper if they have an unexpired conviction, or do not meet the trustworthiness and proper business reputation requirements. These criteria have a broad legal and practical interpretation and cover the association with criminals. Since June 2021, as result of the cooperation and knowledge transfer between the EFSA and EFIU, the fit and proper assessment process is similar to that of the EFSA. The application is verified against the same wide range of sources of information and databases (as described for the EFSA), including EFIU's own records. Potential association with criminals is verified by carrying out background checks on the names and relatives connected with the applicant and identified via Business or Population registries, including by checks against the EFIU's information from STRs, misdemeanour proceedings, archived criminal records.

578. The EFIU also has powers to contact relevant foreign authorities for any information about the applicant or any individuals associated to that applicant, however in practice it does so rarely. This is particularly important in the case of VASPs, where the overall majority of the providers have a board member, shareholder or beneficial owner who are a foreign citizen (84% of the sector in 2022, even after the extensive licence revocations), and about 50% of the VASPs have e-residents amongst the associated persons. Other sectors of concern are the CSP and DPMS sectors, which have an important, but less significant proportion of foreign connection, compared to the VASP sector.

Table N°6.3: EFIU licensing statistics

	2015	2016	2017	2018	2019	2020	2021
Licence applications	88	68	126	1427	1690	1320	232
Withdrawn before formal decision	0	0	1	0	7	0	70
Incl. withdrawals due to fit and proper	-	-	-	-	7	0	33
Negative decisions	1	0	4	94	259	166	25
Incl. negative decisions with a fit and proper element	-	-	-	-	64	41	13
% of non-issuance of a licence (total)	1.1%	0%	3.9%	6.6%	15.7%	12.5%	41%
% of non-issuance of a licence (fit&proper)	-	-	-	-	4.2%	3%	19.8%

579. The number of refusals before 2018 was insignificant. Of the total number of licences refused by the EFIU (549), 21.5% were on fit and proper grounds, mostly due to: (i) lack of AML/CFT knowledge (in 103 cases) and, to a lesser extent, due to (ii) negative information about the natural or legal person (15 cases). In 2019 and 2021, about half of the withdrawals of the applications before a formal assessment were made on fit and proper grounds. The majority were related to the negative information identified by the EFIU, especially in 2021 (24 cases).

580. The most common grounds for refusal are: the certificate of criminal records not being provided; lack of fitness and propriety of the individuals owning, controlling or managing the applicant, including convictions; lacking document; unfit compliance officer; unpaid state fee (specific for FIs); the management of the business not being in Estonia (specific for VASPs).

581. Between 2018 and 2020 there was a significant increase in applicants, the vast majority of these are made up of VASPs. In 2018, out of 1182 received applications made by the VASPs, 58 were refused, in 2019 this number rose to 1519 with 214 refused (64 on fit and proper grounds). In 2020, out of 1234 applications, 155 were refused (41 on fit and proper grounds).

582. This still is a large number of newly authorised entities for the size of the supervisory department of the EFIU (4 people in 2018 and 9-10 in 2019-2020) and it is difficult to surmise that this volume of applications were afforded the scrutiny they were due, considering that an average of between 4 and 5 new authorisations were granted per working day over the year.

583. The licensing process for VASPs lacked robustness, resulting in a large number of entities being licensed which had inadequate systems and procedures, no connection to Estonia and many being misused for criminal purposes. The situation changed in a positive direction in 2021, when as a result of a number of important steps undertaken by the authorities in 2020 and 2021, including legislative amendments, the licensing process for VASPs was overhauled. This is evidenced by the decreased number of applications, greater proportion of licence refusals and application' withdrawals (41%), including on fit and proper grounds (19.8%). In the second half of 2021, only one VASP license was granted.

584. At the time of the on-site visit, the authorities informed the AT that VASPs were subject to a moratorium on licensing in order to give the EFIU the opportunity to review its existing portfolio of authorised VASPs. In March 2022, the licensing regime was further strengthened.

585. The new requirements and the increased capacity enabled the EFIU to revoke a significant share of licenses of unfit entities, mostly VASPs.

Table N°6.4: EFIU statistics on revoked licences

Sectors	2015	2016	2017	2018	2019	2020	2021
VASPs	0	0	1	29	97	1784	329
CSPs	0	5	3	3	2	3	7
DMPSs	0	53	9	3	4	0	7
FIs	0	46	29	25	29	17	27
Pawnshops	0	13	12	4	0	0	0
Total	0	117	54	64	132	1804	370
Incl. revocations due to fit and proper	-	-	-	-	1	4	11

586. The authorities advised that a large share of VASP licences were revoked due to the lack of a connection to Estonia and because of the entities' inactivity. The primary reasons for the 2021 revocations refer to: (i) entity repeatedly fails to follow the precepts of the supervisory authority; (ii) entity has presented falsified data to the EFIU; (iii) entity's compliance officer or members of the management board are not suitable; and (iv) entity has not started providing services within 6 months of licensing.

587. Whilst it is commendable that the EFIU is undertaking these actions and the results of a more compliant industry are now beginning to show and, additionally, the new requirements will prevent such entities being licenced in the future, the fact that so many of these unsuitable entities were licensed in the first place cannot be ignored. The licensing process is intended to stop entities whose compliance officer or management board are not suitable and those which provide false information – so it stands that these firms should never have been licensed in the first place if the licensing process was effective.

588. As at 02 May 2022, there were 369 valid licenses in issue. The EFIU must continue these efforts and remain vigilant regarding the ongoing monitoring for compliance with the entry requirements and detection of criminals and close associates of criminals related to VASPs. This concern is raised by the AT in the context of the increase since 2020 of the foreign requests (69 in 2020, 107 in 2021) in connection to VASPs licensed in Estonia in connection with fraud, ML, drug-related and other predicate crimes.

589. The same concern is applicable in relation to the CSP sector, particularly due to their role as a concentration point for a substantial amount of shell and shelf companies. As pointed out by the recent 2021 SRA of the CSP sector, Estonian companies, including companies founded through the mediation of CSPs, are used in domestic and international crime as shell and buffer companies and, as evidenced from international requests received by the EFIU (18 in 2020, 22 in 2021), the trend to use Estonian companies as shell companies has continued and even intensified.[173] This

[173] Surveys | Financial Intelligence Unit (fiu.ee), SRA on CSPs, 2021, page 3, 5, 16, 42

is also confirmed by the fact that the main reasons for not granting a CSP license is the absence of certificate of criminal records or the actual conviction of the applicant. In two cases, the EFIU revoked the licenses of CSPs, based on the information discovered during supervision, and also in cooperation with the PBGB, which indicated that these entities have been involved with criminal proceedings or were associated with criminals. While these actions are commendable, more rigorous and systematic measures are needed aiming at ensuring that CSPs are not owned by or associated with criminals, or used for criminal purposes. The concerns are also substantiated by the high number of identified unlicensed operating entities and the insufficient supervisory measures applied to the sector.

590. The EFIU conducts measures to identify unlicensed activities mainly by checking the Internet (social media, news agencies, forums, etc.), the information disclosed in the received STRs, FIU-to-FIU cooperation channels and information from potential victims. Nevertheless, the results are not very successful, especially in the most material sectors, such as CSPs. The 2021 risk analysis on CSPs revealed that 40% of the companies that have the characteristics of corporate service providers operate without a valid licence. In three cases, the EFIU initiated misdemeanour proceedings against two natural persons and a legal entity, for providing services without a license (in 2018 and 2019 - 2 cases of unlicensed VASP activity and in 2020, 1 – CSP activity). Considering the explanation above of the EFSA's powers and the restrictive judicial interpretation on this matter, it remains unclear what was the legal basis for the EFIU's actions. Regarding the criminal punishment for unlicensed regulated activity, in the absence of the relevant information on the number of cases referred to the prosecution by the EFIU, the extrapolated results described for the EFSA, indicate an extremely low success rate of successful convictions.

Auditors Oversight Board

591. The Auditors Oversight Board is responsible for licensing statutory auditors in Estonia. Assessments of fitness and propriety of Estonian auditors are focussed primarily on good reputation, conduct, solvency and competence matters. All applicants must make a declaration that they do not have *a conviction for an intentionally committed criminal offence*, however the Board does not independently verify this information. Likewise, the measures do not extend to criminals' associates.

Tax and Customs Board

592. In the case of casinos, the ETCB assesses the fitness and propriety of those applying for a licence to operate a gambling business including casinos. The general process for licensing a gambling firm is a 2-stage process requiring an activity licence and an operator licence. The AML/CFT fitness and propriety element forms part of the activity licence. Much of the focus is on the prudential capitalisation of the business and its financial history, including the applicant's tax behaviour of the last three years. These checks have the effect of informing an assessment as to whether the business' true place of activity is in Estonia, but also whether assets from criminal sources could be used to set up the casino. Therefore, they would be of value in assessing whether the individuals are associates of criminals. The business reputation and trustworthiness of the applicant is checked based on publicly available sources and enquiries made by the ETCB with the EFIU and the PBGB databases. In case of foreign applicants, the foreign authorities are not contacted for additional relevant information.

593. The ETCB processes approximately 3 applications for activity licenses per year on average (although this spiked to 8 in 2021 due to COVID). The power to refuse an application sits with the Board itself, however no licence applications have been formally refused on AML/CFT or integrity grounds.

Chamber of Notaries / Ministry of Justice

594. The Licensing of Notaries is undertaken by the MoJ. There can only be a maximum of 100 notaries authorised at any one time in Estonia, at the time of the onsite there were 88 notaries licensed, 2 of whom were appointed in 2019 and 2020. Most assessment criteria are based on the applicant's experience and qualifications to act as a notary, bankruptcy and whether a person has been removed from public office on disciplinary grounds. The integrity assessments are limited to criminal records check on the individual, but do not extend to associates of that person.

595. The MoJ is empowered to interview applicants and undertake further checks, however there is no evidence of this power being exercised in practice and only the existence of criminal records and bankruptcy is actively verified by the MoJ. In the last 5 years there have been no Notaries referred for disciplinary measures for AML/CFT matters (including suspension for criminal charges) and no notaries applying for appointment were refused or withdrew their application.

Bar Association

596. New members of the BA are required to pass a series of examinations and obtain articles from a law firm before seeking admission to the Bar. A committee of the BA, made up of members of the BA, academics and representatives from the MoJ and 2 judges and 1 state prosecutor, will review the submissions of prospective applicants assessing their competence, experience and criminal record. The fit and proper checks comprise honesty and ethical requirements; a conviction of an intentional criminal offence; deprivation of the rights to be an attorney, judge, prosecutor, notary or entrepreneur; disbarment or removal from the notary practice. The assessment is largely focussed on the competence of the individual to act as an attorney rather than exploring the integrity of the person in any real depth. In practice, the Association also places a degree of reliance on the law firm itself having undertaken sufficient vetting of new applicants. Criminal records checks are done on the individual but do not extend to associates of that person. Certain categories of candidates, such as public prosecutors, judges and notaries, are subject to a simplified examination procedure which is based largely on an interview with the committee of the BA. Since 2014 only a single person has been refused admission to the Bar on integrity grounds.

597. An attorney shall be disbarred in the case of conviction for an intentionally committed criminal offence, or for another criminal offence that renders practicing as an attorney impossible. In the last 5 years, 10 people have been removed as attorneys or have been forced to resign on integrity grounds – 9 of these were for criminal convictions and 1 was an individual who was ultimately not convicted, but the Bar felt there was still sufficient grounds to have them removed for having an *unsuitable background*.

6.2.2. Supervisors' understanding and identification of ML/TF risks

598. Overall, supervisors' identification and understanding of ML/TF is varied, with a better understanding of the ML risks for FI's licensed and supervised by the EFSA and a still evolving understanding regarding higher risk sectors licensed and supervised by the EFIU, such as VASPs and CSPs. In all cases, TF risk understanding appears to be less developed, being assessed as "low" for all FIs and the gambling sector, "average" for CSPs and real estate brokers, "below average" for legal professionals and "high" regarding VASPs.

EFSA (FIs)

599. The EFSA has a good understanding of the ML risks for the financial sector. This is based on a range of information and automated IT-tools, including NRA, SRA, annual off-site questionnaires, monthly updated Risk Dashboard tool and the Risk-based approach model calculator for individual FIs. The available tools started to be developed in 2014-2015, with a more comprehensive and consolidation since 2019. The EFSA also demonstrated the dynamic character of the available tools due to the plans to adjust the risk indicators according to the new ML/TF risks identified by the 2020 NRA and by the 2021 SRA, namely related to CSPs, VASPs and the correspondent relationships with clients who are financial institutions, especially those that also provide virtual asset services.

600. Following the publication of the NRA, the EFSA published its own SRA which identifies the banking and investment sectors to be the highest risk sectors it oversees. This conclusion is largely due to the potential exposure of non-resident customers in those sectors and also the pervasive nature of the sectors within the Estonian financial system. Banking institutions make up the vast majority of the financial sector by assets under management, staff employed and contribution to gross domestic product. Investment business firms make up the third largest sector managing over €1.3bn of assets. Nevertheless, the residual risk in these sectors is perceived as low.

601. TF risk is assessed as "low" in all sectors, despite the cross-border threat and the threat related to the relatively high number of correspondent accounts with the Estonian banks of foreign FIs and VASPs, which use them to serve their own customers, including high-risk businesses. Also, the intelligence available in the country regarding the use of remittance services for TF purposes, does not appear to be taken into account.

602. The results of the Risk-Based Approach model during 2015-2021 regarding the risks in different financial sectors, are the following:

Table N°6.5: Risk rating of FIs – excluding currency exchange offices

Sector	2015	2016	2017	2018	2019	2020	2021
Credit Institutions	Medium	Medium	Low	Medium	Medium	Medium	Medium
Investment Firms	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Small Credit Institutions and Branches	Medium	Medium	Low	Low	Medium	Low	Medium
Credit Institutions and Branches	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Significant Credit Institutions and Branches	Low	Medium	Medium	Medium	Medium	Medium	Medium
Payment Service Providers	Low	Low	Low	Low	Low	Low	Low

Life Insurance Companies	Low	Low	Low	Low	Medium	Low	Low
Branches of Credit Institutions	Low	Low	Low	Medium	Low	Low	Low

603. From the findings of the NRA and the SRA, the in 2021 EFSA has developed a risk-based framework (originating from 2015) which categorises all FI's into 1 of 5 risk levels – very low, low, medium, high and very high risk. The EFSA gathers input to this tool from the findings of the NRA, the SRA, annual off-site questionnaire, input from LEAs and the EFIU. At the time of writing there are no FI's which are rated very high risk and only 2 entities are considered to pose a higher risk. In 2021, based on the EBA guidance on risk-based supervision, the 5 categories were converted into 4: very low risk and low risk - less significant; medium risk - moderately significant; high risk - significant and very high risk - very significant (essentially the low and very low risk brought together). Nevertheless, the five categories still remain and are used by the EFSA for its supervisory activity.

604. According to the RBA Model governance 2020 and 2021 document, before 2021 the model was not applied to each fund management company, creditor or credit intermediary. The reasoning was that fund management companies are either part of banking groups or focus on managing pension funds (considered as posing low risk). Consumer credit loan providers offer loans to private individuals and in small amounts. The risk of these sectors was assessed based on the off-site questionnaires (sent out once in two years). According to the EFSA, the recently renewed off-site questionnaires and increased capacity of the AML Department, would provide a better opportunity for assessing the individual risk ratings for institutions in those sectors.

Table N°6.6: Risk rating of individual FIs

Credit Institutions	High	Medium	Low	Very Low
2015	3	3	10	0
2016	2	5	9	0
2017	1	4	9	1
2018	2	7	4	0
2019	2	7	3	2
2020	0	9	3	1
2021	1	6	7	1

Investment Firms	High	Medium	Low	Very Low
2015	1	2	0	0
2016	1	2	0	0
2017	0	2	1	0
2018	1	0	2	0
2019	1	2	2	0
2020	1	1	3	1
2021	1	1	5	0

Payment Service Provides	High	Medium	Low	Very Low
2015	0	6	4	3
2016	1	3	7	2
2017	0	5	4	1
2018	0	1	5	0
2019	0	2	4	0
2020	0	1	7	3
2021	0	3	8	3

Life Insurance Companies	High	Medium	Low	Very Low
2015	0	1	3	0
2016	0	1	4	0
2017	0	1	4	0
2018	0	2	3	0
2019	0	3	2	0
2020	0	2	3	0
2021	0	1	4	0

605. Despite the available tools for ML/TF risk understanding related to the supervised sectors, the application of the risk methodologies lacks clarity and often lead to assigning a lower risk level for the sectors and individual FIs that would appear to pose a higher level of risk.

606. According to the EFSA's internal guidance, FI's are only deemed "very low risk" if they either do not offer services or where they are, they are limited to a small number of customers (e.g., for consumer credit providers there are 100 or fewer customers).

607. In practice, however, a significant percentage of entities are classified as "very low risk" and many of those do offer services, a good number of whom have over 10,000 customers. Those rated as very low risk are subject to much less scrutiny and supervision than those posing a low, medium or high risk, on the basis that they are very small or not trading. Because many of these entities do not meet the criteria of a "very low risk" entity, the risk-based approach applied to them by the EFSA must be reconsidered to reflect the risks that they actually pose. Many of those FI's risk rated as "very low risk" by the EFSA should be reviewed and re-rated as a higher risk than currently, and the degree of scrutiny and supervision revised accordingly.

608. The risk-based approach is weighted very heavily on location of deposits and payments. The risk monitoring dashboard used by the EFSA is fed by multiple sources of data including routine reporting from obliged entities and payment flows from the Central Bank. The data is reviewed by a team of analysts who identify unusual activity such as payment spikes or dips. Whilst this is an impressive system and provides useful, objective and high-quality quantitative data, the risk-based methodology applied to it appears to give undue weight to the situs of the payments and the residence of the obliged entity's customers.

609. The focus on these risk factors is understandable given the fact that the deficiencies in recent high profile banking scandals stemmed from the non-resident clients of those banks. Although, non-resident clients present a sizable risk factor, other important risk factors in the context of Estonia and which are included in the RBA Methodology should be given appropriate weight, such as the OE's compliance track record, customers involved in higher risk sectors, complex products and multi-layered delivery channels.

610. Reviewing the output of the RBA Model, one bank is rated as posing only a medium risk because of its relatively low volume and value of non-resident deposits and payments. However, at the time of writing, this entity is being prosecuted for multiple deficiencies under the MLTFPA and ML, the AT cannot agree that the EFSA's risk assessment is commensurate with the risks it faces, and the AT's conclusion is that the EFSA's risk-based methodology should include, or give greater weight to, risk factors beyond customer geographical location. Likewise, based on the same metrics, in 2019 four banks were rated with a low and very low risk and in 2020 about half of the total banks were rated as posing very low risk (4 banks) and low risk (3).

611. From interviews with the private sector, a number of higher risk industry sectors are using payment service providers, mostly outside of Estonia for their transactional banking services. This is largely because the banks in Estonia have a reducing appetite for higher risk business. However, the risk persists as many of the foreign payment service providers and VASPs use Estonian banks' correspondent accounts to serve their customers.

612. The AT also observed that most higher risk activity has become concentrated in a small number of service providers, which creates additional challenges for the supervisors than if that risk was more evenly spread.

EFIU

613. Throughout most of the period under review, the EFIU demonstrated a limited understanding of threats and vulnerabilities in the supervised sectors. The reason for this is due to the relatively small number of inspections undertaken and those inspections not being risk based, the AT noted that since 2019, this was beginning to improve, and the 2020 NRA and the 2019 SRA show this improvement. The SRA and the results of the supervisory activities showed that more profound and detailed approach is needed, which led to creating a Risk matrix tool (first version 2020, which is regularly updated). Since 2021, a new obligation for the supervised obliged entities was introduced to make regular reporting to the EFIU. Although it remains unclear what kind of data is planned to be collected, the AT considers the new development as very useful for tool for a more comprehensive understanding of the sectors under supervision.

Table N°6.7: ML/TF risk level based on the 2020 NRA results

Sector	ML Risk Level	TF Risk Level
VASPs	High	High
Financial Institutions	Average	Average
Real estate agents	Average	Average
CSPs	Average	Average
Dealers in precious metals and stones	Below-average	Below-average
Accountants	Below-average	Below-average
Auditors	Below-average	Below-average
Gambling sector	Below-average	Low
Pawnbrokers	Low	Low
Currency exchange	Low	Low

614. The EFIU has recently conducted in-depth research of sectors that have been deemed higher-risk sectors in the NRA and/or in the EFIU internal risk assessments: the assessment of risks related to virtual currency service providers (2020 and more extensive in 2022) and corporate service providers (2021), as well as wider sectors such as the ML/TF risks arising in the Estonian real estate sector and in dealers of precious metals and stones. This will undoubtedly contribute to a better understanding of the high-risk sectors and the AT commends the efforts of the Estonian authorities, particularly of the EFIU, in this respect.

615. During most of the period under review, the VASP sector was not sufficiently regulated, and the supervisory resources were disproportionately low compared to the exceptionally large number of entities operating in the sector, which affected the level of understanding of the ML/TF risks of the VASP sector. The 2022 analysis improved considerably the understanding of the ML/TF risks posed by VASPs. The assessment was based on off-site questionnaires, STR information, FIU-to-FIU information, public information identified about Estonian VASPs, analysis of CSP activities and connection to VASPs and information from LEAs. Nevertheless, the

VASP sector is still characterised by a low level of transparency and a lack of complete risk mapping, as highlighted by the additional risk analysis of the VASPs sector based on the developments in the period 2020-2021.

616. The EFIU does not proactively check whether authorised VASPs (or VASP applicants) are providing services relating to buying, selling or intermediating in the sale of virtual assets which are securities as defined by IOSCO.

617. Regarding the CSP sector, the NRA indicates an average ML/TF risk, the 2021 risk assessment highlights a series of vulnerabilities and features of the sector which indicate a significantly higher ML/TF risk. Although the 2021 risk assessment improved the level of understanding by the supervisor, its comprehensiveness is still affected by a series of factors, *inter alia*, the substantial amount of CSPs operating without a licence, the significant number of licensed CSPs which do not provide corporate services, but are connected with e-residents, the lack of information on whether the Estonian CSPs provide trust services, the weak supervision during the period under review, which is not commensurate with the high-risk appetite if the sector.

618. Both of Estonia's greatest ML/TF threats fall under the supervision of the EFIU and whilst it is clear that the EFIU is developing a better understanding of the risks of these sectors, in particular the VASP sector, further development of its understanding of these risks, particularly as the sectors grow in Estonia and evolve globally, is important.

Chamber of Notaries

619. The CN considers the real estate sector and the transfer of legal entities to be the greatest ML/TF risks facing it. Between 2018 and 2021 these 2 areas made up less than a quarter of notarial activities (in aggregate) – 23% relate to the authentication of real estate transactions whereas less than 1% of activities relate to transactions involving legal persons. Transactions with real estate, where the money is of dubious origin, including cash, accounts a quarter of notaries in their notarized transactions.

Table N°6.8: Notarial activity regarding transactions with real estate and legal persons

	2017		2018		2019		2020		2021	
Total activities	315 704	100%	322 972	100%	328 447	100%	298 433	100%	332 261	100%
Authentication of transaction with real estate	74 219	24%	72 008	22%	73 398	22%	72 005	24%	88155	26%
Transactions involving legal persons	2551	<1%	2635	<1%	2297	<1%	2065	<1%	3022	1%

620. The NRA rates the notarial sector as posing an overall low risk of ML/TF. The main risk typologies that the sector sees are the use of cash in the purchase of real estate or of a company, the involvement of foreign banks or funds coming from a source outside of Estonia and the use or corporate structures with overseas companies.

621. The Chamber's primary source of understanding and assessing the risk of its sector comes from its work with the EFIU and the sharing of information and typologies. The Chamber meets with the EFIU several times per year to discuss emerging risks and typologies as well as a best practice matters.

622. One of the main vulnerabilities identified by the notary sector is the perceived unreliability of the data within the beneficial ownership register. The Chamber considers the main risks facing notaries sit within the real estate sector and notaries may be exposed by extension to being used inadvertently for a money laundering scheme, however its view is that there is no real risk in practice of notaries being used for ML/FT purposes because "they understand their ML/FT risks, the application of CDD and the noticeable participation by notaries in training organised by the EFIU". The Chamber did not explain to the AT how this understanding translated into there "being no real risk".

623. As noted above, the Chamber further considers that the risk of escrow services for property transactions is mitigated because the notary "*has full knowledge of the source of funds*" coming from a bank and undue reliance on those payments having been checked by that bank's own AML/CFT checks.

624. The Chamber was clear that it views its vulnerability as very low without being able to adequately justify that view. During interview the Chamber was not able to explain the risks that it and its sector faces as such the AT is not convinced that the CN has a rounded view of risk of individual entities or the sectors which it supervises.

Bar Association

625. The BA considers the greatest risk facing attorneys is those providing advisory services to VASPs. In the NRA the Estonian Bar considers the greatest ML and TF risk to be cash transactions, however it also notes that the use of cash in Estonia is extremely low so the real risk of this is negligible. The BA considers that the greatest vulnerability facing it is a lack of reliable databases containing information about PEPs which means that it is "*most difficult [for attorneys] to implement control and due diligence measures for PEPs*".

626. Overall, the NRA states that the money laundering and terrorist financing risk for attorneys is low on the basis that Estonian attorneys do not *generally* become involved in legal transactions such as real estate transfer or the transfer of legal entities. This is not an unreasonable conclusion of the inherent risks facing the sector and the evaluation team would largely agree that the inherent risk is lower than most other sectors.

627. However, Estonian attorneys can become involved in transactions which pose a higher risk of money laundering or terrorist financing, such as real estate transactions and corporate structuring (including the sale and purchase of corporate entities). The BA states that in such cases other obliged entities, including notaries and banks, will be involved and so the attorney will rely on those entities to identify any suspicious activity.

6.2.3. Risk-based supervision of compliance with AML/CFT requirements

EFSA

628. The EFSA oversees almost all financial institutions (about 120) in Estonia and so it is responsible for the supervision of a diverse number of sectors requiring a various skill set within its Supervision Departments. The EFSA's Anti-Money Laundering Department is made up of 12 people including its Divisional Head, 4 analysts and 7 others with legal qualifications. Other departments within the EFSA also contribute and have contributed to the AML/CFT supervisory

work. The EFSA was able to demonstrate that currently its staff had the appropriate breadth and depth of skills required to supervise the FIs properly.

629. In terms of its capacity, this was not always the case during the period under review. The resources allocated for the AML/CFT supervisory activities have been increased gradually due to the emerging ML/TF risks related to non-resident business identified mainly since 2014 (from 3 persons in 2013 to 7 persons in 2019). For a substantial period of time, especially during 2014-2018, its resources were overburdened by two high level bank cases and two high-risk PSPs, which required immediate interventions and most of the available resources. In all four cases the licenses were revoked or a prohibition to operate was issued for long-lasting serious breaches (1 case in 2018 and 3 in 2019). Subsequently, this also prevented the authority to intervene earlier in another high-level bank case, which postponed the inspection for the next year.

630. In relation to non-resident ML/TF risks, the EFSA established in 2015 a risk-based model, which was consolidated in 2019 as a Risk Dashboard solution[174] for measuring the ML/TF risks and serves as basis for its risk-based approach supervisory activity. The risk-based model was complemented (since 2019) by the cyclical approach aiming at covering all sectors, irrespective of their risks. Overall, the supervisory circle shall be based on the following indicators: (i) every year for high and very high-risk entities; (ii) every three years for medium risk entities; (iii) every five years for low-risk entities; (iv) only off-site coverage for very low risk entities.

631. Notwithstanding, as it can be seen from the information illustrated by the tables below, the supervisory activity during the period under review may not have always been fully carried out on a risk-sensitive basis.

Table N°6.9: Number of AML/CFT on-site inspections (full and thematic) by the EFSA

Sector	2015	2016	2017	2018	2019	2020	2021
Banks	1	2	2	1	5	2	8
PSPs	0	1	2	2	0	3	0
EMIs	N/A	N/A	N/A	N/A	N/A	0	0
Consumer credit providers	0	0	5	5	0	0	6
Investment firms	0	0	0	0	1	0	2
Fund managers	0	0	0	0	0	0	0
Life insurances	4	0	0	0	0	5	0
Total	5	3	9	8	6	10	16

Table N°6.10: Level of supervisory attention

Sector	2015	2016	2017	2018	2019	2020	2021	Average
Banks	20%	67%	22%	8%	83%	20%	47%	39%
PSPs	0	33%	22%	17%	0	30%	0	25%
EMIs	N/A	N/A	N/A	N/A	N/A	N/A	0	0
Consumer credit providers	0	0	55%	42%	0	0	40%	39%
Investment firms	0	0	0	0	17%	0	13%	12%
Fund managers	0	0	0	33%	0	0	0	33%
Life insurances	80%	0	0	0	0	50%	0	47%

[174] Finantsinspektsioon is introducing a new program for measuring the risk of money laundering | FSA

632. A considerable amount of time is spent on firms which are rated low risk or very low risk such as consumer credit providers or life insurance companies, whereas firms which are rated as posing a higher risk by the EFSA's own risk analysis, such as investment firms, are subject to an insignificant part of the supervisory focus.

633. In spite of the high ML/TF risks posed by the credit institutions during the period 2015-2018, very few on-site inspections were carried: 1-2 inspections per year. It must be noted, however, that these inspections were the most supervisory intensive full-scope inspections commensurate to the risks of the institutions. Nevertheless, not in all cases the resources are allocated for high-risk credit institutions. The AT came across two cases (banks) which would have required more prompt supervisory actions by the EFSA. The Authority informed the AT that the supervisory cycle's principles established in 2019 (see above) will ensure that FIs rated as high risk will be inspected at least once a year. While the initiative is commendable, the effectiveness of this approach depends to a high degree on the accuracy of the assigned risk level for the individual FIs, which is questioned by the AT. On the positive side, since 2019, a more risk sensitive approach to the supervision can be noticed which targeted higher risk sectors.

634. When on-site, the inspection team, typically made up of several personnel from across the EFSA with the relevant skills, will involve the review client records on an intelligence basis as well as a risk-based selection of client entities, this selection will always include the larger clients of the entity or clients with relevant risk profiles, as well as broader statistical sampling. On-site, the EFSA will interview the management board of the obliged entity as well as compliance staff, audit and customer service officers. The EFSA has the power to expand the scope of the inspection or order a separate, parallel inspection if material matters outside of the inspection scope are identified. The on-site inspections, both full scope and themed inspections appear to be overall comprehensive and has sufficient depth to draw meaningful and evidence-based conclusions into its report. Group risk assessment is also considered in supervision, especially after the high-level ML cases involving certain Estonian and Nordic banks. This is exemplified in the joint full-scope onsite inspections described under IO.2.

635. The existing supervisory arrangements between the two main supervisors, the EFSA and EFIU, regarding the entities which are carrying out both financial and VA related services, are impacted by some uncertainties. The AT identified a case of an EFSA licensed entity carrying on additionally VASP activity, which was not acknowledged as such by the supervisor (nor by the entity itself) at the time of the on-site visit and, subsequently, not supervised for that activity. This entity did not appear to have the depth of understanding of the VASP sector that would be expected, nor of the risks that the sector posed to its business. The new services provided by the entity were acknowledged as VASP activity by the supervisor at a later stage and are supervised by the EFSA.

636. In another case identified by the AT, an EFIU licensed VASP was granted additionally an FI licence by the EFSA (EMI). Such situations were not brought to the attention of the AT by the EFSA (nor by the EFIU). Nevertheless, the authorities explained that the FIs which are licensed by the EFSA, and which also undertake VAPS activity are supervised by the EFSA holistically, including the services related to VA. In this case, the entity did not appear to have a clear understanding of which authority would be the designated supervisor and was referring to both authorities – to

the EFIU, in the context of the VASP activity and to the EFSA, in relation to the provided financial services.

EFIU

637. The EFIU is responsible for the supervision of between 10,000 and 11,000 entities with an inspection team of 9 individuals in 2021. As can be seen from the table below, the inspections unit of the EFIU undertakes an average of 30 on-site inspections per year (approximately 0.2% of the total). Both of Estonia's greatest ML/TF risks (VASPs and CSPs) fall under the supervision of the EFIU. Whilst it is clear that the EFIU is developing its capacity, it is still insufficiently resourced to be able to meaningfully inspect the broad breadth and depth of the sector it is responsible for supervising, even on a risk-based approach. Before 2019 (during 2015-2018), the resources were far more limited, about 3-4 persons responsible for the supervision, which raises for the AT even a greater concern regarding the effectiveness of the supervision during the period under review. Desk based supervision procedure is carried out by one person, but on-site supervision is always carried out by at least two officers.

638. Before 2020, the supervisory activity was not conducted on a risk sensitive basis which would take into account the highest-risk sectors, but rather focused on areas triggered by circumstantial factors, such as alerts from STRs, complaints or negative information, or legislative amendments for establishing a lower cash threshold related to AML/CFT obligations, alerts issued by other authorities regarding possible unauthorised activities of the Estonian registered companies in other jurisdictions, increase of real estate market value, etc. In other cases, where the risks were known, i.e., regarding the VASPs sector, the supervisory actions, particularly the on-site inspections, were limited by the fact that most of the service providers did not have a real office in Estonia and did not keep any documents related to the provision of the service.

639. In 2019, the EFIU initiated a sectoral risk assessment, which served as basis for creating a Risk matrix tool which was in use from 2021. As a result of a newly introduced requirement in 2021, OE's will be required to submit reports which are used to improve the Risk Matrix tool and help the EFIU to assess more effectively the ML/TF risks in the sectors under its supervision.

640. The cycle of the inspections established by the EFIU is: high and medium high-risk entities annually, medium risk entities every 3-4 years and medium low entities after five years, low risk entities are supervised generally with off-site inspections. However, as it can be seen from the tables below, this approach was not implemented by the authority before 2021.

Table N°6.11: Number of on-site inspections by the EFIU

Sector	2015	2016	2017	2018	2019	2020	2021
FIs	9	25	1	1	5	3	0
DPMSs	3	2	1	0	0	0	0
Pawnbrokers	34	22	5	0	0	0	3
CSPs	0	4	0	2	0	2	2
VASP	N/A	N/A	0	3	5	6	14
Currency exchange	0	9	0	0	0	0	0
Gambling sector	6	1	0	0	0		0
Traders	6	10	6	0	1	6	4
Accountants	0	0	1	0	0	0	0
Auditors	0	0	0	0	0	5	0
Real estate agents	0	0	0	0	8	10	0
Other	1	7	3	0	1	1	2
TOTAL	59	80	17	6	20	33	25

Table N°6.12: Level of supervisory attention by the EFIU

Sector	2015	2016	2017	2018	2019	2020	2021	Average
FIs	15%	31%	6%	17%	25%	9%	0	17%
DPMSs	5%	3%	6%	0	0	0	0	4%
Pawnbrokers	58%	28%	29%	0	0	0	12%	32%
CSPs	0	5%	0	33%	0	6%	8%	13%
VASPs	N/A	N/A	0	50%	25%	18%	56%	37%
Currency exchange	0	11%	0	0	0	0	0	11%
Gambling sector	10%	1%	0	0	0	0	0	6%
Traders	10%	13%	35%	0	5%	18%	16%	16%
Accountants	0	6%	0	0	0	0	0	6%
Auditors	0	0	0	0	0	15%	0	15%
Real estate agents	0	0	0	0	40%	30%	0	35%
Other	2%	9%	18%	0	5%	3%	8%	7%

641. Over the period under review, it can be noticed that substantially more supervisory efforts (despite the limited resources available) were allocated for lower-risk sectors, compared to higher risk sectors. For example, pawnbrokers, assessed as posing a low risk, and traders (car and art dealers) which have a below-average ML/TF risk according to the NRA, were under much higher supervisory focus, compared to the CSP sector, which is the most material DNFBP sector.

642. Considering the high-risk appetite of the CSPs, their active involvement in establishing around 75% of the VASPs registered in Estonia, their role in establishing non-resident business in Estonia and in concealing the actual controlling structures of the companies, the high ratio of unlicenced entities carrying on CSP activity, as well other aspects identified by the 2021 risk assessment of the CSP sector (e.g., low awareness of the AML/CFT obligations, incomplete risk systems, insufficient implementation of the CDD and reporting obligations), a significantly higher share of the supervisory efforts shall be allocated for this sector. The authorities informed the AT that as a result of three inspections carried out in 2020 and 2021, all three inspected entities surrendered their licenses. This confirms the AT's concerns regarding the CSP sector, and the need of higher supervisory attention.

643. On the positive side, due to the regulatory reforms and increased awareness, the intensity of the supervision of the VASPs has significantly improved and in 2021, together with off-site inspections, constituted about 95% of the total supervisory efforts. Nevertheless, as described under CI 3.2, the EFIU shall expand the focus of the supervision in order to check whether authorised VASPs are providing buying, selling or intermediating in the sale of virtual assets which are securities as defined by IOSCO, as well as shall proactively assess whether VASPs may be undertaking other regulated activities such as services to securities, payment services, electronic money issuance or VASP lending and ensure they are appropriately licensed and supervised.

644. The EFIU's supervisory focus on the real estate sector was commenced only since 2019. This had some positive effect as a number of notifications were submitted by the sector to the EFIU as a result of the supervisory activities. However, considering the identified serious, repeated, and systematic breaches, these efforts shall be continued. With regard to other relatively important sectors, such as DPMS and gambling sectors, the focus and frequency of their inspection, although limited, are considered to be sufficient by the EFIU. This is based on the fact

that the DMPS and gambling sectors are very concentrated and that the biggest entities representing the sectors have been subject to on-site inspections in the last 5 years. Still, having regard the weak understanding of ML/TF risks and superficial controls demonstrated by the entities during the interviews (especially by DPMS'), as well as the expressed needs of more guidelines and feedback from the authorities (gambling operators), a higher supervisory attention shall be paid to these sectors.

Chamber of Notaries

645. The CN aims to undertake periodic supervision on its 88 members. According to the Chamber's procedures, the firms scheduled for an inspection are selected based on the number of notarial acts undertaken in a given year, the proportion and value of real estate transactions and total value of transactions as well as any feedback given by the EFIU, which appears to be on a risk basis.

646. In the course of 2020-2021, due to pandemic, the supervision took form of an offsite questionnaire (extraordinary inspection specifically on AML/CFT issues) which was sent to every notary. For the rest of the period under review, no specific on-site AML/CFT inspections have been performed. However, the AT was informed that the Chamber carried out 5 regular (general) on-site inspections in 2018 and 3 in 2019, which included AML/CFT related topics. Overall, the number of entities inspected in a given year is extremely low and such a small sample size cannot be deemed to give a meaningful evaluation of the sector at large.

Bar Association

647. The BA's inspection team is made up of 1 lawyer and 1 legal assistant who undertake the inspections on 222 law offices. The BA aims to undertake an onsite inspection on 25 law firms per year and in the years 2018 – 2021 this objective was met.

648. It should be noted for context that in Estonia there are 16 law firms which employ 44% of all attorneys in Estonia and it is these 16 firms which undertake the vast majority of activities within the scope of the MLTFPA, such as advising on real estate or corporate structuring. 74% of law offices are single person firms and do not perform tasks which are within the scope of the MLTFPA and primarily carry-on activities such as representing clients in court proceedings.

649. When planning an inspection, the focus is given to the larger firms which are undertaking activities bound by the MLTFPA. Within those larger firms, those selected for inspection are largely random, although may be intelligence led when the Association has relevant information.

650. The BA has introduced a voluntary best practice certification process in which law firms will "apply voluntarily higher standards in their internal procedures" which are then subject to audit. Firms holding this voluntary certificate, having demonstrated appropriate procedures, are generally rated as posing a lower risk and so the BA's inspections will be more focussed on those posing a higher risk.

651. Whilst there is logic to this methodology by focussing on those firms which are undertaking activities within the scope of the MLTFPA, whilst there is some degree of risk basis to the methodology, it cannot be agreed that the supervisor is truly undertaking risk-based supervision within that large sub-set of firms.

6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions

EFSA

652. The EFSA has a broad range of supervisory measures and sanctions in order to ensure the compliance of the FIs under its supervision with the AML/CFT obligations. Nevertheless, it mostly uses remedial supervisory measures to deal with AML/CFT breaches, such as warnings, remediation plans and precepts, including for serious breaches. This is true even for the most material sectors, such as banks and investment firms, which pose a higher ML/TF risk.

653. The precepts are used to restrict certain transactions or lines of businesses until AML/CFT deficiencies are remedied. In the view of the authority, this can be more dissuasive than a fine because this limits the entity from generating revenue from certain profitable business-lines. For example, the EFSA restricted the provision of specific services of a payment institution (2018) or to provide services to new clients in the case of an investment firm (2022).

654. The EFSA also uses alternative means to dissuade FIs, such as setting higher capital requirements for banks that have not met the AML/CFT requirements, therefore restricting the use of capital earned and payment of dividends to shareholders. This has a greater impact for some smaller banks, because it limits their ability to grow and forces them to react more quickly to shortcomings identified.

655. Overall, the EFSA places significant emphasis on the remedial supervisory measures and consider them efficient and often sufficient for having a deterrent effect against future breaches. However, the duration, the seriousness and the repetitive character of the identified AML/CFT violations (mostly those identified before 2020) cannot support this view fully.

656. The banking sector is known for committing serious AML/CFT violations and for its involvement in high profile ML offences, which are currently under criminal investigations by the Estonian and foreign authorities. Notwithstanding, as it can be observed from the Table 6.13, during the period under review, the EFSA imposed a financial sanction only once. Although the successfully applied fine of EUR 1 million in 2020 is considered proportionate and dissuasive in the particular circumstances of the case, and the authority is commended for this, the general application of pecuniary sanctions, especially for serious and long-lasting AML/CFT violations, is considered insufficient by the AT.

657. This might be the result of the particularities of the misdemeanour proceeding pursuant to which the EFSA is empowered to impose fines, while acting as an out-of-court (misdemeanour) proceeding authority. The procedure is complex and denotes a series of limitations. These include: a two-year limitation period (from the moment of committing the AML/CFT violation), high evidentiary standard and complex procedural requirements, as well as a low maximum amount of fines[175] that can be imposed. Therefore, the system in place for applying financial sanctions does not feature the characteristics of an effective, proportionate and dissuasive sanctioning regime (see further details under R.35.1). In this context, the EFSA had already expressed the faced difficulties[176], as well as the need for a more simplified procedure for

[175] Until November 2017, the maximum fine per misdemeanour was Eur 32 000, which was increased to Eur 400 000.

[176] https://www.fi.ee/en/news/estonian-financial-sector-needs-higher-fines-and-faster-legal-proceedings

imposing administrative fines. The current maximum fines are not considered by the authorities to work as an effective deterrent for a breach. This issue was also acknowledged by the NRA 2015, and the subsequent Action Plan (2016-2017) and NRA 2020.

658. In one case, the EFSA reported that the misdemeanour proceedings against a bank, which could have led to imposing a substantial fine, was dropped in favour of criminal proceeding initiated against the entity (as required by the legal framework). The initiation of a criminal proceeding suspends the misdemeanour one. However, given the complexity of the offences under the MLTFPA, the two-year limitation period (from the moment of committing the AML/CFT violation) is insufficient and there have been instances when offences have timed out whilst pending appeal.

659. The following table provides an overview of the remedial actions and sanctions for AML/CFT violations, applied by the EFSA during the period under review, for each supervised sector.

Table N°6.13: Sanctions applied by the EFSA for breaches of AML/CFT obligations

		Banks	Investment firms	PSPs	EMIs	Consumer creditors	Fund managers	Life insurance
2015	Written warning/remediation plan			6		2		
	Precept (demanding/ prohibiting certain actions)	1						
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ compliance officer							
	Withdrawal of a licence							
	Sanctions taken to court							
2016	Written warning/remediation plan	1		3		28	2	
	Precept (demanding/ prohibiting certain actions)							
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ compliance officer							
	Withdrawal of a licence							
	Sanctions taken to court	1						
2017	Written warning/remediation plan	3		2		19	1	1
	Precept (demanding/ prohibiting certain actions)			1				
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ compliance officer							
	Withdrawal of a licence			1[177]				
	Sanctions taken to court	1						
2018	Written warning/remediation plan	2	2	2		6		
	Precept (demanding/ prohibiting certain actions)					1		
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ compliance officer							
	Withdrawal of a licence	1		2				
	Sanctions taken to court			1				
2019	Written warning/remediation plan	4	1		1	4	3	
	Precept (demanding/ prohibiting certain actions)	2						
	Fines/Amount	1 1mln €[178]						
	Management/ fines imposed/ amount							

[177] The PSP withdrew the licence itself
[178] Criminal proceedings are pending for infringements identified in another on-site inspection

	Removal of manager/ Compliance officer	3[179]	2[180]					
	Withdrawal of a licence	1						
	Sanctions taken to court							
2020	Written warning/remediation plan			3	1			2
	Precept (demanding/ prohibiting certain actions)	2						
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ Compliance officer							
	Withdrawal of a licence							
	Sanctions taken to court							
2021	Written warning/remediation plan	5	1			3		
	Precept (demanding/ prohibiting certain actions)	1	1					
	Fines/Amount							
	Management/ fines imposed/ amount							
	Removal of manager/ Compliance officer							
	Withdrawal of a licence							
	Sanctions taken to court							

660. Remediation plans form the overwhelming majority of measures applied by the supervisor to deal with breaches. At least three banks with serious AML/CFT deficiencies, including one large bank, had extensive and long-term remediation plans in place, with measures imposed by the EFSA. Only in one of those cases, the remediation plan proved itself as an effective tool to improve the overall compliance of the entity. Precepts are issued to a lesser degree, and rarely the non-compliance levy for the unimplemented precepts are applied (only once in 2019). The rights to issue precepts are quite extensive and can be used to impose prohibitions, demand termination of certain violations, propose amendments to the organisational structure, impose limitations, etc. In one case, the EFSA issued a precept prohibiting the branch of a foreign bank from operating in Estonia. Other examples when the issued precepts were effective refer to the imposed restrictions on certain transactions, prohibition of new business relationships or termination of certain customers' portfolio. The publication of applied formal measures, such as precepts, also can have a positive effect in terms of dissuasiveness. However, the number of formal measures imposed is low (about 9 precepts issued during 2015-2021). As described above, a fine has been applied in one case to a bank, and there are no cases of imposing a financial penalty to directors or senior managers of the FIs.

661. In some instances, the supervisory actions could be more prompt. Entities have exited the market without being effectively sanctioned for the committed breaches identified by the EFSA (see the case of 2017 regarding a PSP, Table 6.13). It appears that no sanctions are imposed to senior managers and employees of the supervised FIs. For example, at least 4 members of the management board, 1 member of the supervisory board and 2 employees of one bank and one investment firm (2019, Table 6.13) were able to leave the office before their reassessment with the fit and proper requirements and without any sanction being applied to them for the committed breaches. In this case, the EFSA is of the opinion that the desired effect would be achieved by preventing those people to re-enter the market (by applying future fit and proper checks). While such an approach can have an effect to some degree regarding the Estonian

[179] 3 members of the management board and 2 employees left the office in 2020, before fit and proper proceedings started.
[180] 1 member of the management board and 1 member of the supervisory board left the office before fit and proper proceedings started.

financial market, these measures do not have a dissuasive character and the desired effect cannot be ensured in other jurisdictions.

662. The EFSA also has the power to withdraw an FI's license where appropriate and this is considered by the authority to be one of the most significant sanctions available to it. In the case of banks, the competence belongs to the ECB. One Estonian bank lost its license. This was decided by the ECB based on the EFSA's proposal. It is worth mentioning that this was the first case when the proposal for the licence revocation of a credit institution submitted to the ECB was solely based on AML/CFT violations.

Box: Withdrawal of a licence of a bank

This bank was ascertained as risk number two after the branch of another foreign bank in the risk assessments of EFSA. Therefore, the EFSA initiated its first on-site inspection in 2015, which revealed severe shortcomings in AML/CFT risk controls. The inspection was followed by several meetings between the management board of EFSA and the higher management of this bank. One year later – 2016, a precept was issued by the supervisor requiring an immediate rectification of the identified severe breaches. Also that year, the EFSA had expressed its doubts regarding the fitness and propriety of the bank's management and, as a result, the bank changed the supervisory board of the bank (2016).

In 2016, EFSA had cooperation and information exchange with its foreign counterpart from country M regarding information on suspicious transactions involving possible illegal cross-border activity, which were discussed with the bank's management. The media was also describing the AML/CFT breaches as being related to unusual and suspicious schemes and transactions. Allegedly, during 2013-2014, more than 205 million euros of illicit money flowed through the bank's accounts. A follow-up inspection was carried out by the supervisor (in the second half of 2016), which identified that the precepted issued earlier that year was not implemented by the bank.

In 2016, the supervisor from another EU country (L) has decided to prohibit the bank in question from providing financial services on its territory, due to illegal provision of services through a permanent physical presence (a non-authorised branch), demonstrated by numerous facts. The EFSA was informed by the foreign counterpart and as a result carried out, without a prior notification, an ad-hoc inspection at the illegal establishment in country L. The inspection did not result in any imposed sanctions. Nevertheless, a year later (July 2017), an agreement has been reached between the bank and the authorities of the country L, which enabled the bank to continue providing services on the foreign market.

In 2017 the EFSA has repeatedly informed the bank regarding the unimplemented 2016 prescribed measures and initiated a dialogue with the ECB on the removal of the bank's license. This was followed by another on-site visit (required by the ECB) and the change of several members of the management board by the ownership.

Overall, between 2015 and 2017 there were altogether four on-site inspections - three of which AML/CFT specific and one regarding the provision of unauthorised services in another EU jurisdiction.

In March 2018, the ECB, as proposed by EFSA (in February 2018), withdrew the authorisation of this bank to operate as a credit institution due to serious, systemic, and long-lasting AML/CFT breaches.

663. The AT acknowledges the importance of the applied supervisory measures, which led to the revocation of the bank's license on AML/CFT grounds, and which undoubtedly had an important deterrent effect at that time for other market participants. In the same time, the details of the case, together with the publicly available information, point out to a series of weaknesses of the applied supervisory and enforcement measures, which impacted their effectiveness and dissuasiveness. As a result of the four on-site inspections carried out during 2015-2016, only one sanction in the form of a precept was applied in 2016; the precept was issued about one year later after the end of the first on-site inspection (2015); it appears that no levy for the non-

compliance with the 2016 precept was applied; the release/ change of several members of the supervisory and management board by the bank's owners was a clear consequence of the EFSA's measures, however no formal fit and proper reassessment was carried out and no sanctions were imposed to them, despite the existing doubts and the knowledge of the bank's possible involvement in illegal cross-border activity; the same observation is valid for the long-time CEO of the bank who left the position only in 2017 and without any sanctions being applied to the person in question.

664. A key deficiency in the EFSA's sanctioning powers is that they are limited to entities that the EFSA has provided licenses to. Where a person is identified as undertaking financial services without appropriate licensing, the EFSA informs the Prosecutor's Office since providing financial services without a license is a criminal offence. 93% of entities that were identified as undertaking licensable activity were not successfully prosecuted primarily because, although the legal entity is registered in Estonia, the operations were outside the jurisdiction and so such situations are not considered to be in the public interest to prosecute. The effectiveness of the sanctioning system for unlicensed activity requires significant improvement, including by providing additional powers to the supervisors, e.g., to fine those acting without a licence or authorisation, regardless if such activity is carried on within Estonia or elsewhere.

EFIU

665. The EFIU has applied a variety of sanctions during the period under review, such as precepts (including the non-compliance levy) and misdemeanour fines. However, due to their limited number and very low value, including when imposed on OEs representing the most material sectors, such as VASPs, CSPs and real estate agents, it cannot be agreed that those are effective, proportionate or dissuasive. Apart from licence revocations and one precept, no sanctions were applied by the EFIU in 2021. The same concerns regarding the misdemeanour proceedings constraints, as described under the EFSA's application of sanctions, are applicable here.

666. According to the supervisor, during 2018-2020, most of the serious, repeated and systematic breaches were found in the VASP and real estate sectors. The following table provides an overview of the sanctions applied by the EFIU during the period under review.

Table N°6.14: Sanctions applied by the EFIU for breaches of AML/CFT obligations

	2015	2016	2017	2018	2019	2020	2021
Fines (misdemeanour)	€400 (5 pawnshops)	€80 (2 traders) €320 (6 pawnshops)	€760 (4 traders)	€600 (1 natural person/ unlicensed VASP activity)	€15,400 (1 VASP) €600 (1 CSP) €200 (1 natural person/ unlicensed VASP activity)	€220 (2 auditors) €8,000 (1/ unlicensed CSPs activity	-
Total fines	**€400**	**€400**	**€760**	**€600**	**€16,200**	**€8220**	-
Precepts	7 (pawnshops) 3 (casinos)	5 (traders) 5 (pawnshops) 7 (FIs) 1 (currency exchange)	11 (accountants) 5 (currency exchange) 1 (FI)	2 (CSPs) 4 (VASPs) 5 (CSPs) 5 (currency exchange)	5 (real estate) 14 (VASPs) 6 (FIs)	6 (real estate) 2 accountants 3 (VASPs) 1 (enf. agent) 2 (CSPs) 4 (FIs)	1 (art dealer)
Total precepts	**10**	**18**	**16**	**11**	**25**	**18**	**1**

Including precepts with a non-compliance levy	-	-	€5000 (5 currency exchange)	€9000 (3 VASPs) € 15000 (5 currency exchange)	€33,000 (11 VASPs) €1,500 (1 real estate) €12,000 (4 FIs)	€9,000 (3 VASPs) €12,000 (4 FIs)	
Total amount of non-compliance levy	-	-	**€5000**	**€24,000**	**€46,500**	**€21,000**	-
Licence revocations	-	5 (CSPs) 53 (DPMSs) 46 (FIs) 13 (pawnshops)	1 (VASP) 3 (CSPs) 9 (DPMSs) 29 (FIs) 12 (pawnshops)	29 (VASPs) 3 (CSPs) 3 (DPMSs) 25 (FIs) 4 (pawnshops)	97 (VASPs) 2 (CSPs) 4 (DMPSs) 29 (FIs)	1784 (VASPs) 3 (CSPs) 17 (FIs)	329 (VASPs) 7 (CSPs) 7 DPMS 27 (FIs)
Total revoked licenses	-	**117**	**54**	**64**	**132**	**1804**	**370**

667. Precepts are issued by the EFIU to remedy the identified shortcomings which are usually related the application of CDD measures, record keeping and procedural rules requirements, as well as to obtain information from the OEs. The non-compliance levy is widely used, especially during 2018-2020, but primarily for the failure to provide information and not for imposing coercive measures to improve the OEs' compliance. This may explain the relatively low value of the individual levies ranging from EUR 1 000 to EUR 3 000, compared to the established maximum of EUR 5 000 for natural persons and EUR 32 000 legal persons (which can be further increased, as explained under R.35).

668. Unlike the EFSA, the EFIU imposes more frequently misdemeanour fines and in few cases, fines were applied to natural persons (although not senior managers). Notwithstanding, the value of individual fines is extremely low, usually varying from EUR 20 to EUR 200. In two cases, the value increased to EUR 500 and EUR 600, respectively, and the highest fine imposed was EUR 15 000 for severe breaches committed by a VASP.

Box N°6.1: Misdemeanour fine on a VASP for severe infringements

In 2019 the EFIU initiated a full-scope inspection at a VASP. The inspection revealed serious shortcomings regarding all AML/CFT obligations: lack of proper risk assessment; deficiencies related to the rules of procedure, the application of CDD measures, including breach of duty to monitor business relationship. The risk assessment and the application of CDD measures have not been adapted to the new specific business ML/TF risks of the entity. The EFIU started misdemeanour proceedings which finalised with the application of a misdemeanour fine of EUR 15,000 on the legal entity and a EUR 400 fine on its compliance manager. The fines were paid and the VASP ceased its activity.

669. Overall, the level of fines is considered by the AT to be very low and non-dissuasive for all sectors, but especially for higher risk sectors (VASPs, CSPs and real estate agents). This is true particularly in the context of the available maximum fines of up to EUR 1 200 for natural persons and EUR 400 000 for legal persons, which are already considered as non-dissuasive by the authorities. Likewise, they do not appear be proportionate with the severity of the identified breaches, as illustrated by the case example described above.

670. Persistent offenders may be subject to licence revocation. The highest number of revocations was in 2020 (1804), 99% of them were for VASPs. The efforts continued in 2021 with 329 revoked VASP licenses and in 2022 when the overall licensing regime was consolidated. The EFIU views this as an effective sanction because it removes non-compliant entities from market

and economic system of Estonia. While this is true, many of these firms should never have been licensed in the first place (see the analysis under CI 3.1).

671. The EFIU's sanctioning powers of the entities, which are not licensed by the EFIU, but carrying on unlicensed regulated activity, remain unclear. Providing services without a license is a criminal offence and the EFIU is required to report such cases to the Prosecutor's Office. The number of such referrals made by the EFIU remains unknown. However, as explained in the analysis under CI 3.1, the rate of the successfully convicted persons is extremely low. Additionally, although unclear on which basis, in three cases the EFIU imposed a misdemeanour fine on two natural persons and a legal person for carrying on VASP and CSP related activities. The level of fines varies from EUR 200 to EUR 600 for natural persons and EUR 8000 for the legal entity. The latter was paid by the legal entity only partly. These are not considered by the AT to be proportionate or dissuasive. As stated previously, the AT's view is that the effectiveness of the sanctioning system for unlicensed activity requires significant improvement, including by providing additional powers to the supervisors, such as clear powers to impose fines, regardless if the unlicenced activity is carried on within Estonia or elsewhere.

Chamber of Notaries

672. While having a broad range of sanctions at its disposal, the CN has stated that, during the period under review, it has not identified any breaches of AML/CFT requirements in the course of supervision that would be the basis for the initiation of disciplinary proceedings against its members. There is one case of removal from the notary practice as a result of disciplinary procedure, however this was not done on AML/CFT grounds.

Bar Association

673. During the period under review, the BA has not imposed any sanctions as a result of its supervisory activity. Some identified deficiencies were eliminated by the law offices within the given term; therefore, no further actions were required in the opinion of the supervisor.

6.2.5. Impact of supervisory actions on compliance

EFSA

674. Based on the risk assessments and as confirmed by the high-profile ML scandals, the EFSA considers non-resident customers to be the largest single source of AML/CFT risk. To mitigate this risk the EFSA discourages banks from accepting non-resident customers the result of which has seen the number of non-resident customers drop from around 20% of banking customer base to less than 7% between 2014 and 2020, deposits from higher risk jurisdictions have all but disappeared in that time frame. The EFSA has guided some higher risk banks to transform their business models from serving high risk non-resident customers to servicing local customers, including providing services in less densely populated areas.

675. The EFSA has revised its approach to ML and TF including increasing resources within its own AML/CFT department and taking robust action against entities where appropriate. A more recent banking supervisory case in 2019 shows that the EFSA reacted more swiftly and decisively showing that the changes made within the EFSA are having a demonstrable effect.

676. In 2018 the EFSA formed a dedicated AML/CFT department which has 12 staff. Altogether there are 17 FTEs allocated to AML/CFT supervision, which includes staff from other departments of the EFSA. Since that time the number and materiality of breaches identified by the EFSA is largely remaining the same between 2018 and 2021. However, it should be noted that the number and the depth of inspections per year has increased by around 50% over that period. As such the number of deficiencies identified per inspection averages from 1:6 in 2018 to 1:13 in 2021. This suggests that the number of deficiencies across the financial services sector is gradually improving. The most common deficiencies are in collection of adequate CDD, quality of risk assessments and effective internal control systems.

677. Since 2019, the EFSA has annually asked the banking sector about its investments in ML/TF and risk management systems (including the employees the number of staff employed in those roles). Following these meetings, the number of employees responsible for risk management within the firms was increased significantly as was the investments in IT-systems related to AML/CFT and training for staff.

678. Estonia's e-residency program is designed to promote foreign investment by encouraging non-resident customers to establish companies (typically through CSPs) and form business relationships in Estonia. The majority of those taking up e-residency are from Russia, Finland and China. The e-residency program appears to directly conflict with the objectives of the EFSA in discouraging non-resident business.

679. Most banks in Estonia have a very limited appetite for higher risk businesses, including e-residents, VASPs and CSPs because of the risks posed. This lower risk appetite has caused many of these businesses to either bank outside of Estonia, or to use EMIs and PSPs outside of Estonia to conduct their transactional 'banking' services because these foreign service providers have a higher risk appetite than most of the Estonian banking institutions and they are deemed by the private sector not to be subject to the same degree of scrutiny from supervisors. This would imply that the higher risk business is moved outside of Estonia. Nevertheless, many foreign credit institutions, PSPs, EMIs and VASPs have correspondent accounts with Estonian credit institutions (mainly 4 banks) and are using these accounts to serve their own customers, including high-risk businesses, which can also be Estonian.

Table N°6.15: Correspondent relationships with foreign FIs & VASPs

Non-resident customers (FIs and VASPs) of Estonian banks	Number
Banks	92
PSPs and EMIs	96
VASPs	43

680. This move has also meant that the Estonian authorities have very limited visibility of the deposits and payment flows being controlled by Estonian FIs, VASPs and DNFBPs because those flows are within banking and payment institutions outside the Estonian financial system.

EFIU

681. Like the EFSA, the EFIU has also expanded its resources in AML/CFT Supervision in recent years, although not to the same degree. This increase in resources is partly driven by the revised approach to risk modelling and in response to the significant increase in licenced businesses

between 2018 and 2020 – particularly with VASPs. The EFIU has also carried out an outreach program by revising its guidance and meeting with regulated entities.

682. The deficiencies identified by the EFIU are largely in areas of CDD, record keeping, ongoing monitoring and quality of risk assessments. The number and materiality of those deficiencies has remained relatively level since 2019. Based on the number of deficiencies and the spread across the industry sectors, these seem to generally be identified from inspections (both on and off site). This indicated that failings may be rectified by individual firms, however the remedial actions are not being identified or applied across the sectors suggesting that the sectors could benefit from a review of how the EFIU shares trends and aggregated key findings from its inspections with stakeholders.

683. Very few deficiencies were identified for auditors, dealers in precious metals and stones, pawnshops and currency exchange offices. Interviews with those sectors suggested a very weak understanding of ML and TF and superficial controls being applied in practice, so this is more likely a reflection of the fact that those sectors have been subject to few inspections since 2018, rather than an indication of strong compliance in those sectors.

684. In 2019 the EFIU undertook a number of inspections on the real estate sector which identified a number of pervasive and material failings which continued in 2020. The deficiencies were principally concentrated on risk assessments, CDD, identification of PEPs and ongoing monitoring.

685. Between 2017 – 2020 there was evidence of CSPs selling companies to e-residents which had been licensed as VASPs. By having the companies licensed and then the CSP merely executing a change of shareholding and appointment of new directors creating the de-facto effect of bypassing many of the controls of the licensing process. The EFIU recognised this and has moved to stop this activity by revoking the licences of the VASPs which have no clear connection to Estonia and making all changes of control subject to the same process and standard as a new application, however the assessment team has identified evidence that this service is still being offered by a small number of corporate service providers with operations in Estonia.

Chamber of Notaries

686. The CN is of the opinion that all notaries are aware of the due diligence measures they need to apply. Because of the very low number of inspections undertaken in the previous 5 years, and the lack of imposed sanctions, there is insufficient data to conclude that the Chambers actions are having an effect on the compliance of its members. The statistics on STR-reporting shows that the supervisor together with the EFIU is beginning to have a positive impact.

Bar Association

687. The BA has undertaken around 25 inspections on its firms per year (approximately 10% of all firms). A number of deficiencies have been identified based on information submitted to the evaluation team. The deficiencies identified were largely around failures to adopt appropriate internal controls, appoint a responsible person to the board of the firm and undertake appropriate risk assessments.

688. The data provided is in an aggregated form between 2017 and 2021 so the team was unable to extrapolate when the deficiencies were identified and whether the actions of the BA are having an effect on the compliance of its members.

6.2.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks

EFSA

689. The EFSA undertakes a multifaceted approach to promoting AML/CFT awareness to the financial institutions it supervises. This includes the publication of an AML/CFT guidance manual, annual AML/CFT information days, participation in a public-private-partnership forum, participation in sectoral associations and specific guidance through the use of off-site and on-site inspections.

690. The EFSA holds "information days" on an annual basis which are an opportunity for the private sector to meet with the supervisor on a sector-by-sector basis. Recent events have included introducing the NRA and SRA results to the private sector, sanctions updates and other topical matters. The private sector representatives interviewed by the assessment team almost universally reported very positively about the quality of these annual information days.

691. The EFSA also arranges periodic meetings with the FIs under its supervision to discuss general AML/CFT risks, those risks which are more sectoral and risks which are specific to the firm. There are around 60 of these outreach meetings per year.

692. In addition to the information days and periodic sectoral meetings, the EFSA proactively writes to firms through "Dear CEO" letters and via the Public Private Partnership forum to highlight key risks and material matters.

693. A demonstrable consequence of this outreach has been the significant increase in compliance and risk resourcing in the banking sector and a general decrease in the materially of deficiencies. The private sector consistently fed back that it felt it has a good relationship with the EFSA as its supervisor, one of the main reasons for this is the usefulness of the guidance issued by the EFSA and the fact that it is open to enquiries from FIs which have been reported as constructive and useful.

EFIU

694. The EFIU has published several guidance documents which aim to assist entities in complying with their reporting obligations under the MLTFPA. The EFIU has also issued an AML/CFT obligation's specific guidance in April 2022, prior to this no other guidance documents for the implementation AML/CFT obligations are available and the representatives of the private sector indicated in some instances the reliance on the documents issued by foreign authorities (e.g. casinos).

695. The EFIU published guidance about how to make STRs and which of the various reports to use and under what circumstances. The EFIU also increased operational feedback to reporting entities in order to improve the quality of notifications in both an aggregate sectorial level and also to individual firms when material errors were identified in submissions.

696. In recent years, the EFIU has also focussed on reaching out to trade organisations (where available) such as the real estate agent umbrella organisation, the VASP Association and Finance Estonia to offer better engagement and guidance on how to comply with MLTFPA obligations. The feedback from these training sessions was generally positive from those who had received it, although all noted that this was a relatively recent development.

697. Real estate agents have only begun reporting STRs in last 2 years, when interviewed only a few firms appeared to be aware of the training made available by the EFIU. Although all were aware of the published guidance, for some this seemed to be very recent news. The real estate sector is not subject to licensing, and although there is an expectation that real estate agents make themselves known to the EFIU before trading, there is no apparent obligation on them to do so and, from discussion with industry representatives, this lack of obligation is generally understood. As such it is difficult to know the true numbers of estate agents trading in Estonia and the means in which to contact those businesses in order to push training and guidance out to them.

698. The published guidance and training sessions were described as useful sources of relevant information by those entities to whom it was brought directly to the attention of – such as VASPs. However other sectors such as real estate agents, casinos, DPMS, pawnbrokers and CSPs reported little awareness of guidance being available

Chamber of Notaries

699. One of the principal methods of reducing the risk of ML and TF in the notary sector is arranging appropriate training, either by itself or with the support of the EFIU. Apart from one training organised in 2019, the Chamber did not conduct any other trainings of its members between 2018 and 2020 on the basis that the MLTFPA was undergoing a review. There were 3 sessions arranged in 2019 whilst 2020 saw training postponed due to the COVID 19 pandemic. In 2021 AML training seminars were re-started with a focus on the newer requirements of the MLTFPA. The assessment team is not clear as to why the training were halted for a number of years on the basis that the legislation was under review with only some aspects potentially changing. The numbers of inspections are also very limited.

700. The CN has published a step-by-step guide to assist its members to comply with their obligations under the MLTFPA. It has also employed the use of a system called "e-notary" which assists in the due diligence process by reviewing certain public sources such as beneficial ownership register, population register, land register and BR and it also makes automatic queries to the EU sanctions list. The Chamber plans to expand on these systems to introduce a program which would assist the notary assess the threats related to the customer and the transaction and select appropriate due diligence measures based on the degree of risk. At the time of the evaluation this system was very newly brought into operation and so it's effectiveness could not be assessed.

Bar Association

701. The BA has published guidelines for its members which address how its members undertake due diligence and risk assessment on customers is available on the BAs website.

702. The Association arranges for training and conferences for its members, this training is typically provided by the EFIU and external speakers. Most guidance and feedback is given on a reactive basis to enquiries from the members of the Bar and through feedback during on-site inspections.

Overall conclusions on IO.3

703. The licensing process of the FIs by the EFSA is overall quite comprehensive, however, for much of the period under review, the EFIU's procedures were less effective, evident particularly in the VASP sector. The EFIU's actions implemented in 2021 appear to have a positive impact on DNFBPs and VASPs licensing processes. The SRBs assessment processes are much less thorough and undertake a limited assessment of the integrity of their members as shown by how few refusals or application withdrawals there have been since 2016.

704. The EFSA has comprehensive risk analysis tools which facilitate a good understanding of risks across the financial sector. Notwithstanding, the application of the risk methodologies, the EFSA should take into account and give appropriate weighting to all high-risk indicators to avoid assigning lower risk rating as would be expected which has a consequential impact on the effectiveness of the EFSA's supervisory approach. The EFIU's supervisory activity was not carried out on a risk-sensitive basis for the most period under review. This was mainly due to its insufficient institutional capacity and limited understanding of the risks of the supervised sectors. Significant efforts have been made recently to address these weaknesses. The SRBs were able to explain some risks, however the explanations lacked depth or real appreciation of those risks with some matters being dismissed altogether without a convincing rationale.

705. The sanctioning mechanisms features a series of limitations, particularly regarding the ability to effectively impose financial penalties. The main supervisors rely heavily on remedial supervisory measures, such as warnings, remediation plans and licence withdrawal (where possible), and there are cases which would require more prompt supervisory actions. Overall, the applied sanctions cannot be considered to be effective, proportionate and dissuasive.

706. **Estonia is rated as having a moderate level of effectiveness for IO.3.**

7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 5

a) Information on the creation and types of legal persons is publicly available within a single environment, at the State Portal administered by the Estonian Information Systems Authority (e-Business Register), which also contains comprehensive and useful information on the steps to be taken before starting a business.

b) The authorities have taken certain steps towards identification, assessment and understanding of ML/TF vulnerabilities and risk exposure of legal entities. Nevertheless, the current understanding is not sufficient to take into account the existing risks; it lacks systematised and consolidated analyses and conclusions on important determinants and factors of risk, as well as on factually ascertained risks.

c) The measures to prevent misuse of legal persons at the level of companies, OEs, competent authorities and registers do not fully enable availability of adequate, accurate and current BO information.

d) The large share of Estonian companies with e-Residents as their basic or beneficial owners, significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information.

e) Competent authorities have timely access to information available in the registers. Nevertheless, there are no enforceable measures (for supervisors) or practices (for all competent authorities) to obtain basic and BO information from companies and other legal entities.

f) Having regard to the significant presence and activities of non-licensed CSPs, the country has not made appropriate arrangements to raise awareness of obliged entities exposed to relationships with trustees and thus provide for adequate, accurate and current BO information on foreign trusts.

g) There are sanctions available against persons, including shareholders and trustees, companies and obliged entities, which do not comply with information requirements. However, these sanctions are not applied effectively, proportionately and dissuasively.

Recommended Actions

Immediate Outcome 5

a) The current understanding of the risks related to the misuse of legal persons, including those arising from the e-Residency program, should be further developed through, *inter alia*, systematised and consolidated analyses

concluding on important determinants and factors of risk, as well as on factually ascertained risks.

b) The authorities should take specific measures to enhance effectiveness of contributions by different actors, such as companies and OEs, to promote availability of quality basic and BO information.

c) Supervisors should implement targeted activities aimed at ensuring effective implementation of information requirements by FIs, DNFBPs and VASPs, including in their relationships with CSPs and other professionals acting as trustees.

d) The authorities should arrange for conducting ongoing checks to verify company information; implement mechanisms and practices to proactively check the veracity of basic and BO information in the registers.

e) Estonia should implement enforceable measures (for supervisors) and practices (for all competent authorities) to obtain basic and BO information from companies and other legal entities.

f) Sanctions available against persons, including shareholders and trustees, companies and OEs, which do not comply with information requirements, should be applied effectively, proportionately and dissuasively.

707. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R R.24-25, and elements of R.1, 10, 37 and 40.

7.2. Immediate Outcome 5 (Legal Persons and arrangements)

708. The legal instruments regulating creation and types of legal persons include the GPCCA, the COC, the NPAA and the FA, as well as special laws on specific types of legal persons[181]. As described in detail in the technical compliance analysis for R.24, the COC defines five forms of business entities – general partnerships, limited partnerships, public limited companies[182], private limited companies[183] and commercial associations, while the NPAA and the FA define two forms of non-business entities – non-profit associations and foundations. In addition, three types of European companies may be created in Estonia – European public limited liability companies[184], European cooperative societies[185] and European economic interest groupings[186]. The passive legal capacity of business and non-business entities commences as of their entry into, and terminates upon their deletion from, respectively, the CR and the NPAR.

[181] E.g. land improvement associations and apartment associations, whose purpose is not to seek profit, but to govern a part of land or a block of apartments (residential buildings).
[182] The minimum share capital of a public limited company is EUR 25 thousand.
[183] The minimal share capital of a private limited company is EUR 2.5 thousand.
[184] Abbreviated as SE, which may be formed by at least two existing companies originating in different EU countries.
[185] Abbreviated as SCE, which may be formed by five or more individuals or companies based in at least two countries with the EEA.
[186] Abbreviated as EEIG, which may be formed by companies or individuals in accordance with the laws of an EU country.

709. The Registration Department of Tartu County Court is the processor of the CR and the NPAR (collectively called the BR, for which the controller is the MoJ) and, since 7 March 2022, of the BOID (for which the controller is the MoF), in charge of all procedures specified in relevant legal acts. The Center of Registers and Information Systems (CRIS) is the other processor of all mentioned databases, providing the necessary IT infrastructure and technical support. CRIS maintains the web portal e-Business Register, which provides centralised and uniform access to all mentioned, as well as other databases (e.g. the Commercial Pledge Register, the Land Register, the Database of Trade Bans, as well as some fields from other databases containing information on, *inter alia*, amount of paid taxes, taxable turnover, tax arrears etc.). A general overview of the dynamics in creation of legal persons in Estonia over the last five years is provided in Chapter 1 (TableN°1.2: Total number of legal persons per type, as at end of year)

7.2.1. Public availability of information on the creation and types of legal persons and arrangements

710. Information on the creation and types of legal persons is publicly available at the State Portal[187] administered by the Estonian Information Systems Authority. There are two options for registering a business in Estonia – in on-line regime through the e-Business Register, or in physical presence through a notary. General partnerships, limited partnerships, private limited companies, non-profit organizations and foundations can be registered on-line. Public limited companies and commercial associations need to be registered through a notary. The state fee for establishing a legal person vary between EUR 20-200, to which the notary fees would be added in case of using notary services for company formation.

711. The State Portal contains comprehensive and useful information on the steps to be taken before starting a business, such as choosing the area of activity based on the Classification of Economic Activities[188] considering whether it is an area of activity subject to special requirements[189] (e.g. activity licence or submission of a notice to competent authorities). It provides detailed guidance[190] comparing various forms of business entities in terms of differences in the size of the necessary start-up capital, the minimum number of founders, the extent of proprietary liability and management organisation, along with links to applicable legislation and regulations.

712. The e-Business Register portal provides access to the data on all legal persons registered in Estonia within a single environment. The authorities advise that general public can view the data of the companies related to them free-of-charge, by logging into the e-Business Register with their ID card. For all visitors of the portal, data about legal persons is viewable by making a simple query[191], where the reply contains general information (e.g. registry code, legal form, address of registration, address of contact person, status, size of capital, date of registration, period of financial year, date of amending articles of association), names of the persons with the right of representation, areas of activity, tax information (arrears and liability to VAT), information on

[187] https://www.eesti.ee/en/life-events/i-would-like-to-establish-a-company
[188] http://www.rik.ee/en/e-business-registry/emtak-fields-activities
[189] https://www.eesti.ee/en/licences-and-notices-of-economic-activity/business-activity-subject-to-special-requirements/commencement-of-business-in-an-area-of-activity-subject-to-special-requirements/
[190] https://www.eesti.ee/en/doing-business/establishing-a-company/comparison-of-each-form-of-business/
[191] https://ariregister.rik.ee/eng

filed annual reports and other documents submitted to the register, rulings with regard to the company (e.g. penalty payment cautions for non-submission of annual reports), and commercial pledge entries.

713. Further information on the legal person, such as the history of registry card, copies of annual reports, articles of association and documents submitted to the register, information on BOs, as well as visualised data graphically illustrating valid and invalid (i.e. present and past) connections of the subject with all legal persons in the e-Business Register and their relationships with natural persons is available upon a fee up to EUR 2 per query as per a pricelist[192]. In addition, information on foreign companies created in EU Member States is available through the European Business Register[193]. Statistical information on legal persons is also freely available and updated on a monthly basis regarding total number of companies, newly registered, dissolved, bankrupt entities etc.[194] The authorities advise of plans to make almost all data in the e-Business Register free of charge for all users.

714. The authorities advise that since amendments to the Securities Register Maintenance Act and the Commercial Code, which entered into force on 1 January 2007, any persons may get acquainted with the data of the shareholders in possession of more than 10% of the shares in public limited companies, as well as the shareholders of private limited companies registered at the Estonian branch of Nasdaq CSD[195]. Every share registered in Estonia is entered in the Estonian Central Register of Securities (ECRS) on a mandatory basis, covering all shares of public limited companies (since 2003), all units of pension funds (since 2002) and all publicly traded bonds and investment fund units. The ECRS also has information on shares of private limited companies provided on a voluntary basis. The authorities advise that currently information is available about more than 7000 legal entities, including most of the large undertakings in Estonia.

715. The ECRS has extensive legal effect. Rights to securities are deemed applicable with regard to third parties only if such rights are entered in the ECRS. Information is usually submitted to the ECRS via the account operators, which are professional participants in the Estonian securities market (banks, investment firms, management companies) and obliged entities based on the MLTFPA subject to application of CDD and related measures. The authorities advise that in practice almost 90% of the assets are under the custody of three banks. The controller of the ECRS is the MoF, and the processor is the private legal entity Nasdaq CSD. Supervision over the registrar is conducted by EFSA.

716. Estonia's legal system is person-based, meaning that legal arrangements do not exist as entities or vehicles of legal capacity. Estonia is also not a party to the Hague Convention and does not recognise trusts nor other arrangements according to the law. The GPCCA attributes legal capacity to either natural or legal persons and, since trusts do not have such capacity, it is not possible to create or establish an express or any other trust under Estonian law[196]. According to

---

192 https://ariregister.rik.ee/eng/pricelist
193 https://ariregister.rik.ee/eng/ebr
194 https://ariregister.rik.ee/statistics
195 Owned by Nasdaq CSD Group, which operates regional central securities depositories in the Baltics and Iceland, with business presence in Estonia, Iceland, Latvia, and Lithuania.
196 This approach is challenged by, *inter alia*, a publication in Juridica International presenting argumentation in favour of the approach that there are arrangements in the Estonian legal system falling into the category of legal arrangements similar to trusts as defined by the EU AML Directive (and the FATF).

the GPCCA, only natural and legal persons can have civil rights and obligations, and this includes owning property. According to the LOA, contracts can be made only between two or more persons. A contract is interpreted according to the actual common intention of the parties. If such intention differs from the ordinary meaning of the words used in the contract, the common intention of the parties prevails. Hence, if it is stated in the contract that one or more parties are legal arrangements, then the persons who are behind the legal arrangement are the parties of the contract, not the legal arrangement itself, since otherwise the contract cannot have any legal effect (or, alternatively, there is no contract at all due to the fact that no other party can be identified).

717. Provision of "trust and company services", which is defined by the MLTFPA as a licensed activity, comprises *"acting as a trustee or a representative of a civil law partnership, community or legal arrangement, or the appointment of another person to such position"* as a sub-type of corporate services. The authorities advise that they have engaged extensively with licenced CSPs and, in addition, have actively looked for actors that might provide company and trust services with no valid activity license (EFIU analysis of CSPs, 2021). In the course of these engagements the authorities have not obtained information that Estonian CSPs are engaged in the provision of trustee services, although they admit that their presence cannot be excluded.

718. According to the MLTFPA[197], a provider of trust services, whose residence or registered seat is in Estonia, is obligated to gather and maintain with the BR data concerning the settlor, the trustee, the protector (if any), the beneficiary or the class of beneficiaries, and any other person exercising ultimate control over the property of the trust. Moreover, such providers of trust services are required[198] to submit to the BOID – within 30 days upon creation of a trust, becoming a trustee or obtaining temporary right of residence – information regarding the mentioned persons, particularly name, identification code and or registration number and country of registration, as well as full name of the trust, date of its creation, country of incorporation, and contact details. The authorities are not aware of trusts that have the obligation to publish data in Estonia. As of 6 May 2022 no trusts have submitted BO data to BOID, and the authorities have not identified any trustees with the obligation to submit such data.

7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

719. According to the NRA 2021, supervisory authorities[199] have observed an upward trend with the use of Estonian legal persons, especially private limited companies, in money laundering schemes at different stages (i.e., both in predicate offending phase, such as committing fraud, as well as in cover-up activities). This tendency is promoted by the favourable environment (speed, reasonable costs, e-Residency program, etc.) created for establishing private limited companies. Due to their limited liability, it would be easy to exploit such companies for committing predicate offences and ML, after which the company can be abandoned, and a new one created, while also hiding the perpetrator's identity (and connection with suspicious money) by using figurehead board members. At the same time, the authorities conclude that companies with limited liability

[197] Section 76 (1^2) as amended on 2 June 2021and entered into force on 7 March 2022.
[198] Sections 77 (3^3) and (3^4) as amended on 2 June 2021and entered into force on 7 March 2022.
[199] Particularly the EFSA, the CN, the ETCB and the EFIU.

still serve as extremely necessary instruments for civil uses and cannot be waived regardless of the exploitation risk associated with them.

720. The main threats on the misuse of legal persons, as identified by the LEAs and the PO, are the following: a) shell companies established in Estonia and abroad with no real economic activity, used for concealing the actual substance of transactions (e.g. ostensible loan and purchase or sale of assets) and the BOs of companies; b) companies set up for specific transactions, which are liquidated or disposed of after transactions are concluded; c) frontmen used as company managers and, in the case of organised ML, networks of cover enterprises with bank accounts in different countries; d) beneficiaries of the e-Residency program, where persons from third countries become e-Residents of Estonia and create a company in their name, which can later be used to commit criminal offences; and e) so-called "on-line investment platforms" created by companies registered in Estonia, where the platforms and the service providers are located outside Estonia.

721. As described in Chapter 1 of this report, the EFIU's analysis on CSPs (2021) provides some insights into the scale and significance of potential misuse of legal persons. According to the analysis, as of December 2020 approximately 10% of Estonian commercial entities and NPOs (26,349 legal persons) have been registered to 96 addresses (on average, 275 companies per address). These companies are often characterised by numerous indicators of shell enterprises (e.g., nominal directors, lack of employees and declared turnover, and failure to submit annual reports for several consecutive years). Overall, the analysis confirms that Estonia as a jurisdiction is quite vulnerable in regard to corporate transparency and misuse of legal persons for criminal purposes, and concludes that there are many indicators that Estonian companies are used as shell companies in international crime. The market for corporate services in Estonia is very active and a part of the services are clearly targeted at the international market.

722. Among analyses conducted by the authorities for identifying risks related to the misuse of legal persons, the EFSA demonstrates established practices of analysing and risk profiling customer base of credit and financial institutions, assessing existence and effectiveness of relevant risk controls, using tools for monitoring residence structure of depositors in the Estonian financial system, trends in the movement of incoming and outgoing payments to/ from the country. It gathers, through off-site surveillance questionnaires, information on non-resident customers, as well as resident customers with non-resident BOs. According to data provided by the EFSA, as of the end of 2021 non-resident clients and resident clients, whose at least one or all BOs are non-resident, hold a very significant portion in total value of incoming (49.1%) and outgoing cross-border payments (53.6%), in the total turnover of customers' securities in purchase (63.4%) and sales (53.8%) transactions, as well as in the total value of deposits (23.6%).

723. While the assessments and analyses conducted by the authorities provide some useful insights into identified trends and scenarios of misusing Estonian companies, this does not amount to a full-scope identification, assessment and understanding of ML/TF vulnerabilities and risks of legal persons, including a reliable estimate of the extent to which legal persons created in the country can be, or are being, misused for ML/TF. The current understanding of the risks related to the misuse of legal persons lacks systematised and consolidated analyses and conclusions on:

a) Determinants of risk, such as the ease of establishment, oversight structure, transfer of ownership rights, registration and reporting obligations, and interlocking shareholdings/ circular ownership for various types of legal persons;

b) Factors of risk, such as the number/ share of companies owned or managed by formal[200] or informal[201] nominees, beneficially owned by foreigners/ individuals unrelated to the Estonian economy, using complex ownership structure to facilitate hiding of beneficial ownership;

c) Factually ascertained risks, such as qualitative estimates on reliability of information in the BR, involvement of CSPs in the establishment of shelf/shell/buffer companies and their use for laundering domestic and foreign proceeds of crime, empirical data on takeaways from STRs, investigations and convictions, typologies and examples of misusing legal persons in various business models, correlations and causal relations between ML/TF risk exposure and legal form.

724. Accordingly, identification, assessment and understanding of the risk related to the misuse of legal persons is not sufficient to take into account the existing risks deriving from, *inter alia*, the large share of Estonian companies with e-Residents as their basic or beneficial owners, significant involvement of licensed and non-licensed CSPs in company registration processes, especially in relation to e-Residents and VASPs, extensively performing as nominal directors and shareholders.

7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements

725. The authorities advise that the main prerequisite enabling prevention of the misuse of legal persons is the overall transparency of the BR and the BOID. In particular, it is stated that almost 90% of Estonian companies do not have complex ownership structures, as they are directly owned by natural persons. As regards BO structure of Estonian companies, the authorities advise that almost 88% of unique BOs reported to the BOID are residents. Nonetheless, throughout the mutual assessment process the AT has been provided inconsistent and contradictory information on the number, as well as basic and beneficial ownership structure of the companies incorporated in Estonia. This included differences between same or comparable data ranging between few hundreds to several thousands (in case of BO information, above 10 thousand), lack of accurate data especially on the higher-risk clusters of e-Residents and non-residents both in terms of their basic and, more importantly, beneficial ownership of Estonian companies. Accordingly, the AT is not in a position to conclude that the authorities have a reliable view of the subject matter so as to be able to identify, assess and mitigate the risk of misuse of legal persons, particularly that associated with specific types (e.g. private limited companies) and ownership structures (e.g. legally or beneficially owned by e-Residents or non-residents) of companies. This also affects information and estimates provided through various strategic analyses[202], which cannot be considered fully reliable as much as basic and beneficial ownership of Estonian companies is concerned.

[200] E.g., through professional gatekeepers such as company service providers, accountants, legal professionals
[201] E.g., through family members, strawmen
[202] E.g. the NRA (2021), the SRA (2021), the risk assessments of VASPs (2020 and 2022), CSPs (2021), and NPOs (2022).

726. On a related note, according to the calculations of the AT based on data provided by the authorities for the highest risk type of legal persons, i.e. private limited companies, at least 18% of unique natural person shareholders of this type of entities are e-Residents or non-residents. Then, at least 33% of unique legal person shareholders of private limited companies are e-Residents or non-residents, or are affiliated to them (where affiliation is realised through full or partial beneficial ownership in the unique legal person shareholder). Moreover, among BOs of private limited companies, at least 17% are e-Residents or non-residents. Considering that around 80% of the companies incorporated by e-Residents are not economically active in Estonia (and that there is no reliable data on the share of non-active companies incorporated by other non-residents), the AT concludes that a significant part of Estonian companies has the features intrinsic to those incorporated in company formation centers with a lower level of corporate transparency and higher exposure to the risk of being misused for ML/TF. This, in turn, confirms the AT's concerns about the quality of BO information in the country with regard to companies of certain types and ownership structures, as articulated further below in the analysis for this Core Issue.

727. The authorities advise that the burden of detecting foul players lays predominantly on supervisory authorities, FIs and DNFBPs. The AT has considered roles, functions and performance of various actors in the AML/CFT system of Estonia to conclude on the overall effectiveness of the system in preventing misuse of legal persons in the country. This concerns the following actors:

a) Companies, which are required to: 1) submit basic ownership information to the BR and update such information whenever changes occur; and 2) gather and retain data on their BOs, including information on their right of ownership or methods of exercising control, and report such data to the BOID for informative purposes. Shareholders or members of the company must provide the management board with all information known to them about the BO. Upon any changes of the status of the beneficial ownership, it is the company's duty to inform the BOID, i.e., to make the changes into the BOID within 30 days of learning that the BO has changed.

b) OEs, which are required[203] to obtain and maintain basic and BO information in the course of CDD measures and, whenever they identify discrepancies with the BO information published in the BOID, notify these to the registrar within a reasonable time, by attaching information or documents that show the difference. The authorities advise that the Estonian wording of "within a reasonable time" calls for OEs not to delay notifications without a reason.

c) Supervisory authorities, which are tasked to check compliance of OEs with basic and BO information requirements, request remediation of shortcomings and, where appropriate, apply sanctions for non-compliance, and may cross-check their findings on the outcomes of CDD measures applied by OEs with the data published in the BR or the BOID.

d) Other competent authorities (the Prosecutor's Office, the ISS[204], the PBGB and the ETCB), which may use the e-Arrest system[205] within the scope of formal criminal investigations to request from connected credit institutions (8 of 15 as of the on-site visit) information on

[203] Section 20 (2^4) as amended on 2 June 2021and entered into force on 7 March 2022.
[204] The ISS can also access the system prior to initiation of criminal proceedings.
[205] https://www.rik.ee/en/other-services/e-arrest

account holders and safe-deposit box lessees, including on authorised persons and BOs (see the analysis under IO.6 for further details).

e) Registers, which: 1) consider technical and structural accuracy of basic information filed by companies, maintain such information and updates to it; 2) receive and maintain BO information filed by companies, notify them about discrepancies of BO information as reported by OEs, propose addressing such discrepancies within 10 working days by providing additional information and proof to the register, or changing the BO accordingly.

728. To enhance compliance of **companies** with information requirements, the COC requires that, if at least half of the management board of a company is located outside Estonia or another EU member state, the company must designate a contact person to receive procedural documents and other communication from the registers. The authorities inform that in such cases only a notary, advocate, law office, sworn auditor, audit firm, tax representative or TCSP may be designated a contact person, whose address shall be considered the address of the company. Nonetheless, as described in the analysis for IO.1 and confirmed in the EFIU analysis of CSPs[206], the requirements of contact person and address are easily circumvented by appointing nominal management and obtaining a formal address in Estonia, including through the services of CSPs and other professionals. Other than this, the assessment team has not been provided information on measures aimed at effective implementation and enforcement of information requirements by companies.

729. With regard to measures taken by or through **OEs**, one should mention that while all companies set up in Estonia are required to have share capital, there is no requirement for the capital to be deposited in an Estonian bank subject to AML/CFT supervision. In contrary, the amendment to the COC effective from January 2019 has removed the requirement for private limited companies to use an Estonian bank account when registering share capital. Therefore, BO information would not be available from banks regarding Estonian companies, which do not have business relationships with local banks. In this regard, the authorities have provided the number of resident legal entities that are clients of Estonian banks (around 298 thousand), which cannot be directly compared with the number of all legal entities in the BR (around 302 thousand) so as to conclude that almost all Estonian legal entities have a local bank account, insofar as one company may have business relationships with more than one bank, etc. A positive feature of the system is that some entries to the registers (on average, around 8 thousand per annum) are conducted via notaries, specifically by foreign individuals who do not have access to Estonian e-services and in case of public limited companies. While this constitutes an additional opportunity for verifying BO information as far as the mentioned type of companies is concerned, its impact on the quality of BO information regarding the most frequently used private limited companies would not be significant as these are predominantly created through e-services and/or mediated by CSPs with a low level of AML/CFT compliance.

730. As to the reporting of discrepancies of BO information to the registers, due to the very recent introduction of the relevant requirement around 40 reports have been filed as of the time of the on-site visit. In addition, the EFIU has received the following number of STRs from OEs referring to possible differences in the BO information: 7 in 2019, 32 in 2020, and 29 in 2021, mainly regarding non-resident companies, which is a very low figure given the significant number

[206] https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#money-laundering-ris

of legal entities nominally and beneficially owned by non-residents that are customers of financial and non-financial institutions of Estonia. Overall, the requirement for OEs to report to the BOID discrepancies of beneficial ownership data entered into force since 7 March 2022, and it is premature to conclude on the effectiveness of its implementation towards contributing to enhanced quality of BO information.

731. As regards efforts of **supervisory authorities** towards prevention of misuse of legal persons, the EFSA has demonstrated certain activities aimed at understanding the size and significance of the cluster of FIs' customers, with regard to whom identification of beneficial ownership is more challenging (e.g., customers related to the non-resident business[207]). The EFSA advises that inspections have identified only a very limited number of breaches of the BO-related obligations (over 2018-2020, only 3 of the total 25 inspections in banks and other FIs have identified such breaches) and usually they have either ended with a written warning or a precept. This is not commensurate to the difficulties reported by FIs in ensuring proper verification of BO data due to, *inter alia*, discrepancies in the BOID and unavailability of data in foreign registries (see the analysis under IO.3 for further details), the current level of population of the BOID[208], the higher risk exposure of non-resident legal entities and e-Residents, as well as the significant involvement of licensed and non-licensed CSPs in company registration processes. As to other OEs supervised by the EFIU and the SRBs, there are facts and indications of a low level of compliance with AML/CFT requirements in general, and information requirements in particular, by most of the supervised entities, especially CSPs and VASPs, as described in Chapter 1 of this report, and there is no comprehensive information on the outcomes of relevant supervisory interventions.

732. Regarding the role of **other competent authorities** in contributing to the availability of quality basic and BO information in the country and thus preventing misuse of legal persons, the ETCB controls the accuracy of the data in the BR exceptionally for tax purposes, i.e., for the availability of financial statements and tax returns of the legal persons included in its control samples, which are composed using parameters unrelated to the risk of ML or TF. Other competent authorities do not report of any mechanisms or practices to proactively check, or otherwise contribute to enhancing the quality of information in the BR and the BOID.

733. As to the **registers** and their role in effective implementation of information requirements, the authorities are of the opinion that the overall quality of the BR is good, and the visibility and transparency of true owners (i.e. legal ownership) is very good and easily accessible, including through the advanced visualisation tools available in the BR. While noting that legal ownership does not necessarily amount to beneficial (or true, as the authorities call it) ownership, during the meetings with the representatives of the registers the assessment team received confirmation that the software implemented by the CRIS provides only for technical and structural accuracy checks of submitted information to ensure that required fields are not left empty or contain inappropriate data. Unless there are irregularities with the submitted documents or the natural person has been deprived of the right to engage in enterprise by a court judgment, the legal entity

[207] Legal persons are considered to be related to non-resident business if they are: (i) e-resident, (ii) resident with at least one beneficial owner being a non-resident, and (ii) non-resident legal persons.
[208] As it is highly unlikely that companies, which failed to provide BO information to the BOID, would provide accurate and reliable information to banks or other financial institutions.

would be registered. For Estonian nationals, the system also enables cross-checks with other databases (e.g., the Population Database) to ensure correctness of personal identification data. Overall, there is a high degree of reliance on the proper implementation of legal obligations by the authorised persons (e.g., directors, members of the management board) of the company to ensure provision of reliable information. No ongoing checks are made to identify changes in terms of the shareholders and the managers of the company.

734. As regards the newly established BOID operational since 7 March 2022, the authorities inform that it has been populated to around 86% due to the migration of existing BO data from the BR. Data in the BOID has informative effect (unlike the entries in the BR, which have legal effect). The guidelines on who are considered BOs have been issued and published on the web page of MoF and CR[209]. In case of changes in the submitted data, the company should submit updated data via the CRIS information system not later than within 30 days after learning of such changes. In the absence of changes in the BO data, the company certifies correctness of the data upon submission of the annual report.[210] As of 29 September 2021, there are 37 769 entities that are obliged to submit BO data to the register, but have not done so. This means, that around 10% of Estonian companies, which would be forced to submit any BO data in order to be able to comply with the annual reporting requirement, would have little or no need or incentives to do so. In relation to this, the authorities advise that the number of non-reporting entities has been decreasing mainly due to two factors: first, submission of BO data is a precondition for incorporating a new company, and second, non-submission of BO data would eventually result in deletion of the company from the BR (a measure reportedly applied to around 30 thousand companies over the last five years). Within the last two months prior to the on-site visit, the BOID has sent 62 notifications to legal persons informing that correctness of the BO data submitted by them has been put in doubt. The authorities advise that these notifications were triggered by discrepancy reports from OEs, which does not reconcile with the number of such reports (around 40) as of the time of the on-site visit.

735. Overall, information submitted to all registers is checked for availability (but not substance) of annual reports to be provided by companies. The authorities advise that entries to the registers are checked against EU and UN sanctions lists, as well as the domestic lists of persons prohibited to do business, and where the registrar cannot decide whether the hit is a false or true positive, additional inquiries are made to the EFIU. Nonetheless, the lack of information on the number of hits and inquiries to the EFIU within the period under consideration does not enable conclusions about effectiveness of these practices. Other than this, the processors do not have any mechanisms or practices in place to proactively check the veracity of basic and BO information. In particular, there are no triggers to initiate testing or verification of accuracy of information, and no actions are taken in case there are doubts about veracity of information, except offering the company to update BO information, which has no legal effect. The large share of Estonian

[209] https://www.rahandusministeerium.ee/system/files_force/document_files/juhis_tegeliku_kasusaaja_tuvastamise ks_inglise_keeles.pdf?download=1

[210] The system produces automatic pop-up notifications to the legal persons once a year. Every legal person would get the pop-up notification if they try to submit annual reports, or have not updated or certified the BO data for one year. It means that all the legal persons get the notifications on regular basis, and it does not depend on whether or not the BO data has been submitted, because the legal entities have also the obligation to keep the BO data updated. All legal entities that have the obligation and are at least one year old receive a notification. Accordingly, annual notifications go to around 256 thousand legal entities during submission of annual reports or due to some other reasons.

companies with e-Residents as their basic or beneficial owners[211], significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information. The registers have no mechanisms or practice for systematic monitoring of instances when legal persons are set up at the same address, by the same person, have the same manager or BO, and for taking relevant preventive or mitigation measures.

736. The authorities inform that new regulation will enter into force on 1 January 2023 to enhance the supervisory role of the Tartu County Court as the registrar of the BR and the BOID. In particular, the registrar will control legal persons contact information, and if the legal person has not been contacted through the given contacts, the registrar may add a note of that to the register, which will be deleted when the registrar successfully contacts the legal person. This will supplement the current powers of the registrar to terminate a legal person, if the articles of association of the company do not contain provisions required by law or are in significant conflict with the law, if the management board of the company does not comply with the requirements of the law, if the company has not designated a contact person, or has failed to submit the annual report. The assessment team considers that all these measures, while with certain positive effect on technical compliance with information requirements, would have little or no effect in terms of substantial compliance with BO information requirements, unless appropriate tools and practices are implemented to ensure the quality of that information.

737. As to special measures to enhance transparency of legal persons, Estonia has prohibited OEs to establish a business relationship or make a transaction with a person, whose capital consists of **bearer shares** or other bearer securities to the extent of more than 10%. In any case, those customers are considered high risk, with mandatory application of EDD measures. The authorities advise that supervisory interventions have not identified any business relationships with such legal persons.

738. The authorities inform that since 2002, only shares registered in the Central Register of Securities are permitted in Estonia. Pursuant to the law, all public limited companies that had issued bearer shares had to convert them into registered shares by 31 December 2001 at the latest. There is court practice[212] resolving that any actions with bearer shares after that date did not confer any rights on the acquirer over the bearer share and the rights of the registered shareholders prevailed, as confirmed by the Supreme Court.

739. Among further specific measures aimed enhanced transparency of legal persons, the authorities advise that the legal system of Estonia does not provide for **nominee directors** and, according to the COC, if the management board of a company does not comply with the requirements of the law or the articles of association, the registrar shall set a term for remedying non-compliance. Every named director would be held liable if their fiduciary duties are neglected. However, this would not prevent the existence of arrangements whereby one natural person formally acts as a director on behalf of another person, although this would be illegal. In reality, as described in Chapter 1 of this report, as well as in the analysis for IO.1, appointment of nominee

[211] As of the end of 2021, e-Residents had established around 21.9 thousand companies in Estonia (8% of all companies), of which only around 4.6 thousand (3% of all active companies) are among economically active companies.
[212] https://www.riigikohus.ee/lahendid?asjaNr=3-2-1-116-08

directors and shareholders has been practiced among licensed and non-licensed CSPs, some of whom are identified as legal and beneficial owners of hundreds or thousands of companies registered in the BR.

7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

740. The **information in the e-Business Register** is accessible free of charge for OEs, competent authorities and courts. For all other interested parties, certain information is accessible free of charge, while detailed data through advanced queries and visualisation tools can be obtained for a fee as per a pricelist (see the details in the analysis for Core Issue 5.1 above). Furthermore, the EFIU, the EFSA, the Prosecutor's Office and the LEAs have unrestricted access to the BO information in cases, where BOs or their representatives have legally applied for the limitation of access to submitted data (e.g., where public access to such data would expose the BO to a disproportionately high risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation)[213]. On a related note, the PBGB and the ETCB advice of operative measures conducted for identification of real BOs of companies, which occasionally result in discovering non-actual information in the e-Business Register (i.e., the real BO is someone else than the person registered in the BOID). Nonetheless, the authorities advise that availability and accuracy of information in the e-Business Register has been improving over the last years due to, *inter alia*, establishing submission of BO data as a precondition for incorporating a new company, deleting from the register companies with missing BO information and, more recently, implementing the new system for reporting discrepancies of BO information by OEs.

741. Regarding access to **information maintained by OEs**, the EFIU is authorised to request and obtain information from any obliged entity in Estonia, and the EFSA has similar powers regarding its supervised entities, i.e., credit and financial institutions. Other competent authorities, such as the Prosecutor's Office, ISS[214], the PBGB and the ETCB, may use the e-Arrest system within the scope of formal criminal investigations to request from connected credit institutions (8 of 15 as of the on-site visit) information on account holders and safe-deposit box lessees, including on authorised persons and BOs (see the analysis under IO.6 for further details). According to the statistics provided by the authorities, within the period 2020-2022 (first four months) the ETCB has made 17 inquiries on BOs, the PBGB – 568 inquiries, and the EFIU – 833 inquiries.

742. The Action Plan developed on the basis of the NRA 2021 findings and endorsed in July 2021 defines the high priority issue related to the MoJ and the LEA access of information as *"it takes too much time to obtain information from credit institutions in criminal proceedings"* with implementation deadline of 2022-2024. To deal with this issue, it establishes to develop the electronic environment and its successor, so that they are used by all banks and payment institutions operating in Estonia, and the quality of the information received is improved. The authorities have not provided further details of the issue identified by the NRA and the Action Plan, and up-to-date information on the implementation of the respective activity.

---

[213] As defined in MLTFPA Section 79[2] (1)
[214] The ISS can also access the system prior to initiation of criminal proceedings.

743. As regards access to **information held by companies**, the MLTFPA[215] establishes that to perform the duties arising from the law, the EFIU has the right to receive information from, *inter alia*, third parties "based on a compliance notice". The EFIU interprets this provision as authorisation for it to request through a precept information from any third party not regulated under the MLTFPA, including companies. However, since non-compliance with such precept has no legal consequences, this article has never been enforced (the EFIU advises that it has requested and received information from third parties, but is not in a position to provide relevant statistics). Other authorities, while confirming availability of mechanisms in criminal, misdemeanour or tax proceedings, do not refer to established practices (as demonstrated through relevant statistics) for obtaining basic and BO information from companies and other legal entities.

744. As to the use of **open-source information**, the EFIU advises of using commercial databases with global and regional coverage, data from leaks, other public information and databases to understand company data and relationships.

745. As regards the extent to which **adequate, accurate and current** basic and BO information on legal persons is available in the country and, therefore, accessible for the competent authorities, the assessment team considers that the measures to prevent misuse of legal persons at the level of companies, obliged entities, competent authorities and registers, as described in the analysis for Core Issue 5.3 above, do not fully enable availability of adequate, accurate and current BO information.

7.2.5. Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

746. As described under the analysis for Core Issue 5.1, Estonia's legal system is person-based, meaning that legal arrangements do not exist as entities or vehicles of legal capacity, and it is not possible to create or establish an express or any other trust under Estonian law. Provision of trustee services, as defined by the MLTFPA, is a sub-type of corporate services, and the authorities' extensive engagement with licensed CSPs, as well as efforts aimed at identifying non-licensed CSPs have not resulted in finding any entities providing trustee services.

747. Nonetheless, having regard to the significant presence and activities of non-licensed CSPs (see the relevant sections in Chapter 1, as well as the analysis for IO.1), which makes Estonia different in this aspect from comparable jurisdictions, the assessment team considers that the country has not made relevant arrangements – at least in the form of specific guidance, training and other targeted awareness raising activities for the obliged entities exposed to relationships with CSPs and other professionals acting as trustees – to improve the understanding of the respective requirements and thus providing for adequate, accurate and current BO information on foreign trusts.

[215] Section 58 (1) as amended on 21 November 2020 and entered into force on 1 January 2021

7.2.6. Effectiveness, proportionality and dissuasiveness of sanctions

748. With regard to information requirements applicable to **shareholders and trustees**, according to the MLTFPA[216] the penalty imposable on a shareholder or a trustee for the failure to submit details of the BO, or to report on a change of the details, or to knowingly submit false information, where it has caused a situation in which the OE cannot apply the due diligence measures related to identifying BOs, as well as understanding ownership and control structure of the customer, is a fine of up to 300 fine units[217]. The penalty for the same act committed by a legal person is a fine of up to EUR 32 000. Hence, application of this sanctioning measure is limited to situations whereby non-compliance of shareholders and trustees with information requirements has caused inability of the OE to apply CDD measures. This sanctioning measure has never been applied to a natural or legal person.

749. As to information requirements applicable to **companies**, according to the COC[218] the registrar may impose a fine on an undertaking and any other person, who fails to submit information provided by law or submits incorrect information to the registrar, regardless of whether or not such information is subject to entry in the register. If a person fails to submit information to the registrar within the term prescribed by law, the registrar may impose a fine on the person without first issuing the ruling of warning specified in the CCP. The fine is imposed in the amount specified in the CCP, but no less than EUR 200. In determining the amount of a fine, the court takes the financial situation of the person and other circumstances into consideration. The authorities have provided the following information on the number and amount of fines imposed on and settled by natural and legal persons for the violation of these requirements.

Table N°7.1: Number and amounts of fines imposed on companies[219]

Year	Total number of fines imposed	Total number of fines imposed for failure to submit annual report	Total amount of fines imposed (EUR)	Total amount of fines imposed for failure to provide annual report (EUR)	Total amount of fines collected (EUR)	Total amount of fines collected for failure to provide annual report (EUR)
2017	309	195	68,300	41,100	23,900	17,100
2018	248	149	55,800	30,900	24,300	17,800
2019	331	222	74,500	46,100	21,000	14,700
2020	120	61	32,000	15,000	10,700	7,800
2021	10,642	10,444	2,377,400	2,325,000	399,200	382,600

750. As one can see in the table above, the average amount of imposed and collected fines is around EUR 235, which is slightly above the minimum threshold established by the law. Then, in 2021 there is an abrupt increase in the number and amount of imposed sanctions. Around 98% of these fines are imposed for the failure to submit the annual report, which indeed has a supportive role in promoting provision of BO information (as the system requires to fill in missing BO data, or confirm accuracy of the available data, in order to permit submission of the annual

[216] Section 95(1) as amended on 10 July 2020 and entered into force on 20 July 2020; Section 95(2) as amended on 17 November 2017 and entered into force on 1 January 2019
[217] According to Penal Code Section 47(1), a fine unit is the base amount of a fine and is equal to EUR 4.
[218] Section 71
[219] Data for 2015-2016 is not available

report). Nevertheless, factual collection rates of all fines and those imposed for the failure to submit an annual report are low, respectively at 17% and 16% in 2020. This means that pecuniary fines as a sanctioning measure to promote compliance with BO requirements are not effectively enforced with regard to companies. Additionally, it is not clear why fines have not been imposed on all entities that are obliged to submit BO data to the register, but have not done so (as of 29 September 2021, there are 37,769 such entities).

751. In addition, knowing submission of false data to the registrar is punishable pursuant to the Penal Code[220] by a fine of up to 300 fine units or by detention. The penalty for the same act committed by a legal person is punishable by a pecuniary punishment. Moreover, submission of incorrect information to registrar is punishable by a pecuniary punishment or imprisonment for up to two years. The authorities refer to a total of 197 instances of applying this sanction over the period 2017-2021, without further details of these statistics (e.g., the circumstances and nature of ascertained infringements, the initiation of misdemeanour proceedings, the types of applied sanctions (e.g., penalty or detention), and the amount of imposed and settled penalties).

752. With regard to information requirements applicable to **obliged entities**, the MLTFPA[221] defines that the penalty for the breach by an OE or its management board member or an employee of the duty to identify and verify the identity of customers, their authorised representatives and BOs is a fine of up to 300 fine units or detention. The penalty for the same act committed by a legal person is a fine of up to EUR 400 thousand.

753. The EFSA advises that this sanctioning measure has been applied only once in 2020 at the amount of EUR 250 thousand in respect of a bank for the breach of the duty to identify BO over the period 2017-2019[222]. Hence, within the period under review (2015-2021) the EFSA has conducted 65 on-site (full and thematic) inspections along with a large number of off-site supervisory interventions, which resulted in application of the legally defined pecuniary sanction for the failure to meet information requirements in respect of one bank only. This confirms the AT's conclusion about over-reliance of the supervisors on other remedial supervisory measures, such as warnings, remediation plans and precepts, thus lessening the dissuasive effect of the sanctioning regime.

754. A similar situation is observed with the obliged entities supervised by the EFIU, which reports about 23 precepts issued over the period under review due to, *inter alia*, shortcomings related to BO requirements. This means that, for example, 28 on-site inspections of VASPs and 10 on-site inspections of CSPs have not identified any breaches of the respective obligations to secure application of at least the minimum amount of the pecuniary fine established by the MLTFPA. For further details on the shortcomings of the sanctioning regime available for the obliged entities see the analysis under IO.3.

755. Hence, the assessment team considers that Estonia does not apply sanctions, that are fully effective, proportionate and dissuasive, against persons who do not comply with the information requirements.

Overall conclusions on IO.5

[220] Sections 280 and 281
[221] Sections 84 and 85
[222] Relevant information is available on the EFSA website.

756. Information on the creation and types of legal persons is publicly available, along with comprehensive and useful information on the steps to be taken before starting a business. The e-Business Register portal provides access to the data on all legal persons registered in Estonia within a single environment. The authorities have taken certain steps towards identification, assessment and understanding of ML/TF vulnerabilities and risk exposure of legal entities. Nevertheless, the current understanding lacks systematised and consolidated analyses and conclusions on important determinants and factors of risk, as well as on factually ascertained risks.

757. Measures to prevent misuse of legal persons at the level of companies, OEs, competent authorities and registers do not fully enable availability of adequate, accurate and current BO information in the country. The large share of Estonian companies with e-Residents as their basic or BOs, significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information. These deficiencies are to a certain extent mitigated by measures such as the newly implemented requirement for OEs to report discrepancies of BO information to the BOID, and linking provision of BO information with the obligatory submission of annual reports by companies. There are some measures in place to obtain basic and BO information from OEs. Nonetheless, there are no enforceable measures (for supervisors) or practices (for all competent authorities) to obtain basic and BO information from companies. Estonia does not apply sanctions, that are fully effective, proportionate and dissuasive, against persons who do not comply with the information requirements.

758. **Estonia is rated as having a Moderate level of effectiveness for IO.5.**

8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 2

a) Estonia provides MLA and extradition to EU and non-EU MS based on international treaties and domestic legislation in a constructive way. The MoJ is the central authority for the processing MLA requests from non-EU MSs, while the OPG is responsible for requests coming from the EU MS. Both authorities use case management systems and general guidelines to achieve prioritisation and timely execution of the received requests to some extent. Estonia has reserved the right to refuse assistance due to the principle of dual criminality, which hinders cooperation with non-EU jurisdictions.

b) Estonia seeks MLA to pursue ML/TF and predicate offense investigations to some extent. There are few requests sent regarding seizing assets in foreign jurisdiction, despite the fact that in majority of cases (especially ML) assets are moved abroad. There is no information on the number of requests sent regarding confiscation of assets in foreign countries. No TF related extradition requests were recorded despite the fact that in all ongoing TF investigations defendants were outside of Estonia, hindering effectiveness of the investigations.

c) The extent to which other forms of international cooperation is sought and provided differs between authorities. While the EFIU seeks and provides international cooperation using various channels of communication when working on the AML/CFT cases, such cooperation is not established within their supervisory role. The PBGB uses various established mechanisms such as EUROPOL, INTERPOL and CARIN for their international cooperation and the ETCB mainly liaison officers. The EFSA collaborates closely with its counterparts through supervisory colleges and joint onsite inspections.

d) Estonia provides basic and beneficial ownership information. Deficiencies identified under IO.5 regarding accuracy of basic and BO information may hinder effectiveness of such cooperation.

Recommended Actions

Immediate Outcome 2

a) Estonia should not make dual criminality a condition when rendering MLA at least for requests which do not involve coercive measures, in accordance with the FATF Methodology.

b) Estonia should more proactively seek international cooperation in order to pursue ML, as well as to support ongoing TF investigations. Particular attention should be given to seeking assistance regarding seizure and confiscation of

assets moved abroad, mindful the fact that most proceeds are moved through Estonia to foreign jurisdictions.

c) The EFIU as supervisor should proactively cooperate to obtain all appropriate information when licensing and supervising, especially VASPs and CSPs.

d) Estonia should broaden the scope of the existing guidelines for MLA by introducing clear indicators for prioritisations of incoming requests. Such guidelines should be made available to all LEAs.

e) Estonia should apply measures to ensure that the effectiveness of provided cooperation (MLA and other forms of international cooperation) is not hindered by the issues concerning deficiencies in maintaining BO information as identified in IO.5.

f) Estonia should introduce a system to maintain comprehensive statistics on international cooperation by all competent authorities (e.g., number of outgoing requests executed, pending, refused, numbers on incoming and outgoing requests for all LEAs when using informal cooperation in AML/CFT related matters).

759. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

8.2. Immediate Outcome 2 (International Cooperation)

760. International cooperation is particularly important for Estonia, given its risk profile, geographical location, and the fact that the majority of criminal cases have an international component (ML, TF, fraud, drug trafficking, trafficking in human beings, etc.). Estonia made the reservation to the European Convention on Mutual Assistance in Criminal Matters (ETS no. 030), reserving the right to refuse cooperation in a case when the request concerns an act that is not considered an offence under Estonian laws.

8.2.1. Providing constructive and timely MLA and extradition

761. In Estonia, prioritisation and timely execution of MLA and extradition requests is ensured to some extent.

762. Estonia provides MLA based on international treaties, conventions, the principle of reciprocity and the EU legislative framework implemented in the CCP (Chapter 19). There are different procedures in place depending on whether the request is coming from EU or non-EU MS.

763. Jurisdictions that provided input related to the provision of MLA by Estonian authorities for ML/TF-related cases reported, in general, a good quality of co-operation responses.

764. The MoJ is the central authority for receiving MLA requests coming from non-EU jurisdictions and assigning them to the OPG or LEAs for execution. It is tasked with verification of the incoming requests, whether they meet necessary requirements. The MoJ has a separate unit

responsible for the coordination and organisation of mutual legal assistance in criminal matters employing two officials to deal with the subject matter.

765. The MoJ handles and monitors MLA requests through the digital management system. Deadlines, prioritisation, and urgency remarks must be registered manually in the system, and it is a manual process for following up on requests. When a request is disseminated to the competent authority for execution, MoJ can no longer follow stages of the execution of the requests but can set some priorities and the request is open until manually marked as executed. The OPG and the PBGB have access to the MoJ case management system and other LEAs uses their own systems.

766. The OPG is the central authority for receiving requests from EU MS – European Investigative Orders (EIO) and uses the same case management system as for MLA requests. Depending on the nature of the request, it is scrutinised and executed by different competent prosecutors. The OPG dedicated three officials to regularly monitor the progress and timeliness of the incoming requests waiting for execution.

767. Authorities advised that prioritisation is based on the deadlines incorporated in the national legislation for certain investigative actions, as well as on the OPG guideline used by both the MoJ and the OPG. Once the request is received, deadline for examination of the request is set up to 7 days and the final decision whether the request is possible to execute shall be made within 30 days. Not all investigative actions that can be subject to MLA have set deadlines in the national legislation and in those cases, authorities use criteria set in the guideline to prioritise requests. The guideline itself is very general and emphasises following indicators to be used when determining priority in execution: (i) request relates to freezing order, (ii) requesting state indicates that request is urgent; (iii) request is connected to a serious crime (drug related offence, serious ML/TF) or (iv) request is related to the ongoing criminal proceeding in Estonia. While such guidelines can provide some prioritisation, it lacks details and comprehensives to determine the level of urgency amid requests falling under the same category of prioritisation. In addition, it should be noted that none of the LEAs are familiar with the indicators for prioritisation and timely executions.

768. Over the reporting period the MoJ received 672 MLA requests for ML predicate offences from non-EU jurisdictions (see table below) mostly from Russia, Belarus, UK and the USA. The most common predicate offences for which assistance was requested were fraud, followed by drug offences, tax-crimes, and cybercrime. Authorities handled requests between 40-100 days, which appears to be reasonable. The scope of the requests was outlined by the authorities as investigative measures, such as hearing witnesses or defendants, providing documents (including bank account-related data), etc.

769. In Estonia, the legislation does not require fulfilment of the dual criminality principle when rendering assistance. Nevertheless, execution of MLA requests in respect to both, coercive and non-coercive measures, is affected by the reservation made by Estonia to the European Convention on Mutual Assistance in Criminal Matters, i.e., the right to refuse cooperation in case when the request concerns an act which is not considered an offence in Estonia. It was observed that authorities used the right to refuse cooperation based on the lack of dual criminality in proceeds generating offences, especially fraud. The refusal rate of incoming requests related to such offences in 2017 and 2020 reached 23% and 33% respectively, and those requests were not

pertained to coercive measures. During other years (2015-2016 and 2018-2021) refusal rate was lower, approximately between 12-23% of incoming requests. Notwithstanding, AT did not come across refusals for ML and TF offences due to the lack of dual criminality. Authorities advised that they do not refuse assistance in all cases due to the lack of dual criminality, however, it is unclear based on which criteria, and under which circumstances, this principle will be used as reason for not rendering assistance.

770. Estonia received 3 139 EIOs related to proceeds generating offences. The authorities indicated that requests received from EU MSs were of a better quality, comparing to those received from non-EU jurisdictions. Timelines for execution of EIOs are shorter, and the refusal rate of EIOs is considerably lower, since dual criminality is not a prerequisite when providing assistance to the EU MSs.

Table N°8.1: Incoming MLA request for predicate offences (from EU MS and non-EU jurisdictions)

	2015		2016		2017		2018		2019		2020		2021	
	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO
Received	75	127	71	409	63	363	97	341	88	535	146	518	132	846
Executed	63	127	57	400	48	348	82	336	74	532	80	497	102	812
Refused	12	0	14	9	15	15	15	5	14	3	49	3	17	3
Approx. Time	80 days	50 days	80 days	50 days	80 days	80 days	90 days	60 days	80 days	50 days	100 days	50 days	73 days	43 days

771. The number of requests received for ML offence has been steadily increasing over the past two years especially from EU Member States. Majority of requests were coming from Finland, which accounted for approximately 27% of the incoming requests. Authorities advised that Estonia is one of the EU-countries, due to their close economic ties, where proceeds of predicate offences committed in Finland are laundered. The remaining requests came mostly from Lithuania and Germany. The time for execution of EIO is considered to be adequate, and the percentage of the refusals is within one digit.

Table N°8.2: Number of incoming MLA requests for ML/TF offence (non-EU jurisdictions)

	2015		2016		2017		2018		2019		2020		2021	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Received	7	0	12	0	11	0	17	2	14	1	31	0	26	0
Executed	7	0	10	0	8	0	15	2	14	0	30	0	25	0
Refused	0	0	1	0	3	0	2	0	0	0	1	0	0	0
Approx. Time	60 days	60 days	60 days	0	60 days	0	59 days	119 days	85 days	-	148 days	0	99 days	0

Table N°8.3: Number of incoming EIO requests for ML/TF offences (EU Member States)

	2015		2016		2017		2018		2019		2020		2021	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Received	61	0	37	0	61	0	36	0	65	0	132	0	121	0
Executed	60	0	33	0	58	0	36	0	65	0	128	0	115	0
Refused	1	0	4	0	3	0	0	0	0	0	0	0	0	0
Approx. Time	50 days	0	50 days	0	43 days	0	40 days	0	45 days	0	53 days	0	53 days	0

772. Throughout the reporting period Estonia received two requests pertain to terrorism and terrorism related offences and three requests regarding TF. Authorities indicated that they did not experience any difficulty when executing such requests. All requests were received from non-

EU Member States and no refusals were recorded. Nevertheless, one of the requests is still pending since the it relates to hearing of defendant who does not reside in Estonia.

773. Legal framework, as it is explained under R.38, allows for cooperation on seizure and confiscation of assets. Estonia provides a wide range of assistance in asset recovery cases, including in identifying, tracing, restraining and confiscating assets. In total, 70 requests for seizing of assets were received and additional 72 request for confiscation, out of which majority was for predicate offences such as drug trafficking, fraud, theft, and tax evasion. International requests regarding seizure and confiscation were executed between 10-117 days, depending on the nature of the request. The average time for execution has improved since 2018. There have been 37 requests, which were impossible to execute, and 21 requests were refused. The reasons for refusal are (i) the property belonged to third party, not related to the criminal offence, (ii) no property, assets or income was located in Estonia, and (iii) there was no legal basis to size and confiscate instrumentalities during 2015-2016[223]. However, authorities did not provide what were the circumstances of the requests which made them impossible to execute.

Box N°8.1: Foreign request for confiscation

In 2016, Estonia received two requests related to confiscation of property located in Estonia. Both confiscation requests were related to ML and computer crime offences that were committed in the foreign country by individuals residing in Estonia. For both requests, Estonian authorities conducted search and seizure of property, comprised of cash, 1 kg of pure gold, money on bank accounts, as well as car and an apartment. Estonian courts recognised the requests and ordered confiscation of property in the amount of EUR 197 685 and USD 41 679. Confiscated property has been shared with foreign country.

Cooperation with neighbouring country

In 2020 Estonia received a confiscation request regarding criminal proceeds deriving from tax crimes committed in the country F. The perpetrator, a national of country F, used different scheme and incorporated a company in Estonia to whose bank account the funds were transferred. Estonian court recognised the confiscation order and EUR 155 870 has been confiscated. Confiscated money was shared equally between Estonia and the country F.

Table N°8.4: Number of incoming requests for seizure

	2015		2016		2017		2018		2019		2020		2021	
	ML	Other[224]	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other
Received	2	1	4	0	3	1	4	8	2	7	2	13	2	21
Executed	2	1	3	0	3	0	2	5	1	0	0	4	0	9
Refused	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Impossible to execute	0	0	1	0	0	1	0	3	1	6	1	9	2	12

Table N°8.5: Number of incoming requests for confiscation

	2015		2016		2017		2018		2019		2020		2021	
	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other
Received	2	8	2	30	0	4	0	2	0	7	0	9	0	8
Executed	1	5	2	23	0	4	0	2	0	3	0	6	0	5
Refused	1	3	0	7	0	0	0	0	0	3	0	3	0	3

[223] In 2017, legalisation was changed, and this does not represent any more the impediment when providing assistance in criminal matters.
[224] Other- other proceeds generating offences

Impossible to execute	0	0	0	0	0	0	0	0	0	1	0	0	0	0

Extradition

774. In Estonia, there is no absolute prohibition to extradite nationals. The extradition is subject to procedures in accordance with the *Acquis Communautaire* of the EU, other international treaties, or bilateral agreements. The majority of requests are coming from EU member states and the simplified procedure through a European Arrest Warrant (EAW) is applied. Extradition requests are usually related to predicate offences such as fraud, drug and tax-related offences.

Table N°8.6: Number of incoming requests for extradition (from EU and non-EU countries)

	2015		2016		2017		2018		2019		2020		2021	
	EXT[225]	**EAW**	**EXT**	**EAW**	**EXT**	**EAW**	**EXT**	**EAW**	**EXT**	**EAW**	**EXT**	**EAW**	**EXT**	**EAW**
Received	5	46	3	33	8	39	12	45	7	35	4	24	4	29
Executed	3	40	1	29	2	36	9	37	3	33	2	23	0	29
Refused	1	6	2	4	2	1	0	1	0	2	1	1	0	0
Approx. Time	180 days	20 days	60 days	20 days	60 days	20 days	200 days	60 days	240 days	30 days	60 days	20 days	-	20 days

775. There have been six requests for extradition for the ML offence during the assessment period. All requests were from EU-Member States. Authorities executed five requests, and one was revoked.

776. There has been one TF related extradition which was executed. Nevertheless, one terrorism related extradition request from 2018 is still pending due to the complexity of the case which involves politically motivated activities of the defendant. Estonia is still assessing the request and its factual circumstances, which raises concern on the effectiveness of the execution of the request related to such a serious offence.

Box N°8.2: TF extradition

In 2018, Estonia received an extradition request from one country in relation to the drug- and TF offences. The arrested person was suspected of financing Taliban organisation with the money received from drug trafficking offences. He came to Estonia to meet with the alleged accomplice and since the crimes were not related to Estonia, he was extradited.

777. It is observed from the table above that there are still pending extradition requests from both EU and non-EU countries related to predicate offences. Authorities explained that the main reason is that the person could not be located in Estonia. Also, in pending EAW cases, Estonian court has decided to surrender the persons to the issuing state. However, due to a sentence for other criminal acts in Estonia, the actual extraditions have been postponed until the prison sentences are served.[226]

8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

778. Given the risk and context of Estonia, many ML, TF and predicate offences have a transnational element. While authorities recognised foreign predicate offences as being the biggest threat for ML, assistance is sought to some extent.

[225] EXT- requests received for extradition from non-EU MSs

[226] Council Framework Decision of June 2002 on the EAW and the surrender procedures between Member States (2002/584/JHA), art. 24.1. CoCP, art. 440 é contrario.

779. The GPO recognises the importance of seeking international assistance in ML and associated predicates with transnational element by outlining this issue in the Manual for MLA. While existence of such manual is welcomed, usefulness of it cannot be assessed since it was not provided to the AT. It is unclear whether such manual is available to all LEAs.

Table N°8.7: Number of outgoing MLA requests for predicate offence (EU MS and non-EU jurisdictions)

	2015		2016		2017		2018		2019		2020		2021	
	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO	MLA	EIO
Sent	17	123	28	208	28	177	32	189	64	243	80	261	73	290
Executed	16	123	22	208	27	171	27	187	51	235	59	241	43	260
Refused	1	0	1	0	1	0	2	0	2	0	1	0	1	0

780. It can be observed from the table above that Estonia is more often seeking MLA from the EU MS and there is slight increase of outgoing requests in the recent years, which indicates Estonia's proactivity when dealing with international crimes. Most of the requests were addressed to Finland, Latvia, Lithuania, and Germany, which is considered to be in line with the risk profile of the country, even though authorities did not assess risk related to geographical exposure. MLA requests were usually related to fraud, computer fraud and tax evasion.

781. Regarding requests sent to the non-EU jurisdictions, even though there are very few refusals, there are still some pending requests (for example in 2017 - 8 requests, in 2019- 31 requests, and in 2020-35 requests have not been executed). Most of the requests were sent to Russia, Belarus and Moldova. Authorities advised that they arranged meetings with the foreign counterparts once the request had not been executed in due time, but limited results have been achieved so far.

782. There is an increase in the number of requests sent for ML offence (especially in 2019 and 2020). Comparing total number of ML investigations conducted in Estonia and number of outgoing MLA requests, it can be concluded that authorities use international cooperation to pursue ML. Nevertheless, it should be noted that there might be a number of outgoing requests sent only in one criminal investigation, e.g., in large-scale ML investigations (see IO.7, Bank D and Bank S case examples).

Table N°8.8: Number of outgoing MLA requests for ML/TF offence (non-EU jurisdictions)

	2015		2016		2017		2018		2019		2020		2021	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Sent	9	6	26	2	21	0	14	0	40	0	52	0	49	0
Executed	9	6	23	2	19	0	14	0	40	0	48	0	43	0
Refused	3	0	0	0	2	0	0	0	0	0	0	0	0	0

Table N°8.9: Number of outgoing EIO requests for ML/TF offence (EU MS)

	2015		2016		2017		2018		2019		2020		2021	
	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF	ML	TF
Sent	9	6	26	2	21	0	14	0	40	0	52	0	49	0
Executed	9	6	23	2	19	0	14	0	40	0	48	0	43	0
Refused	0	0	2	0	0	0	0	0	0	0	4	0	0	0

783. Estonia sent 12 MLA requests related to TF and all of them were executed. The majority pertain to the criminal investigation in Khalilov and Manko case, and the rest of them are sent within the ongoing criminal investigations (see IO.9).

784. Despite the fact that a huge portion of proceeds of crime has been moved abroad, there have been few requests for assistance in seizing of assets. As it is shown in the table below, the majority of requests regarding the ML offence, were sent in 2021, which coincides with the activities undertaken in the case "Bank D" (see IO.7). Authorities did not provide information on the number of requests sent for confiscation order and therefore it cannot be concluded that they actively seek cooperation in order to confiscate proceeds moved abroad.

Table N°8.10: Number of outgoing requests for seizure

	2015		2016		2017		2018		2019		2020		2021	
	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other	ML	Other
Sent	0	2	0	3	1	4	1	0	2	4	0	7	13	5
Executed	0	2	0	3	1	3	1	0	2	2	0	4	7	5
Refused	0	0	0	0	0	0	0	0	0	2	0	3	4	0

785. Joint Investigative Teams are used when investigating complex cases with an international component. Authorities indicated that since 2015 Estonia has participated in 28 JIT-s, out of which 13 were formed for ML offence. Some of the complex ML cases that are under investigation include JIT (see "Bank D" and "Butterfly" cases under IO.7). Nevertheless, there is no information on the number of the JITs formed based on the Estonia's initiative.

Extradition

786. Estonia has asked for extradition for predicate offences in most cases from EU Member States (see table below). Several requests have not been executed since the person was not located in the requesting country. The requests for extradition are mostly addressed to Finland, Latvia, Lithuania, and Germany. The fact that majority of requests were executed, it demonstrates a good quality of the requests filled by Estonian authorities. No TF-related extradition requests were recorded. This raises concerns, since authorities advised that criminal investigations are pending because the defendants are in another jurisdictions (see IO.9). ML related extradition requests are also rare considering international character of those cases.

Table N°8.11: Number of outgoing requests for extradition

	2015		2016		2017		2018		2019		2020		2021	
	EXT[227]	EAW	EXT	EAW	EXT	EAW	EXT	EAW	EXT	EAW	EXT	EAW	EXT	EAW
Issued[228]	1	100	2	97	3	87	3	92	4	103	7	77	3	58
Sent	1	53	2	49	3	53	3	46	4	50	7	53	2	23
Executed	1	53	0	49	0	53	1	46	1	50	3	50	0	22
Refused	0	0	0	0	0	0	0	0	1	0	0	0	0	1

8.2.3. Seeking other forms of international cooperation for AML/CFT purposes

The EFIU

787. The EFIU attaches importance to seeking cooperation from foreign FIUs in ML/TF related cases. The information is exchanged through the EGMONT Secure Web (ESW) and FIU.net. In addition, the EFIU has signed 28 MoUs with its foreign counterparts in order to strengthen

[227] EXT- requests received for extradition from non-EU member states
[228] Sent includes EAWs issued by Estonia and not necessary sent to the receiving MS. The request is marked as sent as soon it is inserted in the SIS system as an EAW.

cooperation with jurisdictions that require such instrument for establishing a framework for international cooperation.

788. The EFIU cooperation is focused on seeking information relevant to transactions. Authorities provided the number of requests sent to counterparts in different geographical regions (see table below) and the majority is addressed to EU MS, which is in accordance with the risk profile of the country. When it comes to seeking cooperation within EU MS the largest number of requests were sent to: Latvia, Lithuania, Germany through FIU.net (around 61%) and ESW (around 37%). It can be observed that there is a steady increase in the number of requests over the year, which confirms authorities' commitment to seek information from the foreign counterparts. However, there is lack of information spontaneously shared with the foreign counterparts (see table 8.13)

Table N°8.12: EFIU - number of outgoing requests for 2016-2021

Region	2016	2017	2018	2019	2020	2021	Total
EU	47	101	98	137	286	153	**822**
CIS (+ UA, TM)	21	32	16	55	43	14	**181**
Europe (excl. EU, CIS)	7	16	19	27	36	25	**130**
Asia	4	8	5	11	21	2	**51**
America	3	7	1	12	9	2	**34**
Africa	0	2	1	1	2	1	**7**
Oceania	2	1	1	1	1	0	**6**
Total	**84**	**167**	**141**	**244**	**398**	**197**	**1231**

Table N°8.13: EFIU - the total number of outgoing requests per country 2015-2021

Country	Request sent	Spontaneous dissemination sent
Latvia	171	9
Lithuania	127	10
Russia	94	14
Germany	83	4
Ukraine	72	17
Poland	72	3
Finland	65	8
UK	64	8
Czech Republic	35	3

789. Despite the fact that there is no clear division on the number of the requests sent for ML and TF purposes, from the discussions with the authorities it can be concluded that the EFIU sought assistance in TF related matters in eight occasions. Considering the authorities' understanding of the TF threats and vulnerabilities, as well as the number of reports submitted by the OEs it cannot be concluded that the EFIU actively seeks cooperation in TF related matters.

790. The EFIU efforts in international cooperation can be observed through the prism of the numbers of the request sent to foreign counterparts in order to support ongoing work of LEAs especially when conducting financial investigations. This form of cooperation is assessed as useful since it can help LEA's further approach when identifying and investigating crimes with transnational element and proceeds moved from and to abroad.

Table N°8.14. EFIU – number of outgoing requests to foreign FIUs to support the criminal or intelligence investigations by LEAs[229]

	2018	2019	2020	2021	Total
Assistance in cases of TF-suspicion	3	0	3	2	8
Financial investigation and other assistance in criminal matters	18	33	81	52	184
Total number of requests on behalf of LEAs	21	33	84	54	202

The PBGB

791. Informal cooperation by the PBGB is operated through various channels such as INTERPOL's 24/7 and EUROPOL's SIENA information exchange channels and cooperation tools. As seen in the table below, the PBGB does actively request information in ML-related cases. There is a huge discrepancy between the number of ML requests sent, and actual ML criminal cases investigated by the PBGB, the latter being low. Authorities explained that in most of the instances multiple requests are sent with respect to a single case, including requests seeking very simple information which can clarify certain issues and help them formulate more comprehensive requests. In general, there are few refusals, based on the fact that the foreign jurisdiction did not possess requested information, which serves as an indicator of the quality of the outgoing requests.

Table N°8.15: PBGB - Number of outgoing ML request

Year	2015	2016	2017	2018	2019	2020	2021	Total
Number	192	224	327	505	776	1216	563	3803

792. In addition, the PBGB also seeks information related to other crimes, mostly pertains to drug trafficking, thefts and robberies, which is not in line with the country's ML threat.

793. The ARO also exchange information when tracing proceeds of crime. Considering Estonia's risk and context (being transit country for foreign proceeds of crime) the number of outgoing requests appears modest, especially in ML related cases (in 2021 only 9 out of 47 requests pertain to ML offence). The majority of ARO's requests were sent to Latvia and Finland, and the most common predicate offence was fraud, which is in line with the country's ML threats.

Table N°8.16: ARO - Number of outgoing requests for information

Year	Requests sent	Average response time (days)	Requests with interim responses
2015	27	61	7
2016	27	38	1
2017	20	36	8
2018	14	23	3
2019	23	12	7
2020	47	29	5
2021	41	21	14

[229] Statistics were provided only for 2018-2021

The ETCB

794. The ETCB has an international cooperation department for tax and custom matters consisting of six designated officials. As a way of informal cooperation, the ETCB has a liaison officer at Europol and a Finnish Customs liaison officer is located at the ETCB which allows for exchange of information in tax related matters, as well as for AML/CFT purposes, when needed. The ETCB also has a seconded customs attaché in Brussels. There is an Intelligence Department within the ETCB, which exchanges information on customs and tax related violations within several cooperation formats, both with internal and external partners. The ETCB participates in EMPACT activities (European Multidisciplinary Platform Against Criminal Threats). Nevertheless, authorities did not present information to demonstrate the effectiveness of such cooperation for AML/CFT purposes.

The EFSA

795. As the main supervisor of the Estonian FIs, the EFSA seeks information on the market entry controls and supervision of the OEs under its competences. The EFSA has three main permanent mechanisms to cooperate with their counterparts: on the basis of MoUs; through supervisory colleges; and in Nordic-Baltic cooperation framework. The EFSA has signed MoUs with Swedish, Finnish, Latvian, Lithuanian, Danish and German supervisory authorities, as well as with supervisors from several non-EU jurisdictions[230]. The Nordic-Baltic cooperation framework has been especially reinforced due to the banking sector ownership structure in Estonia and aims at enhancing the cooperation between the supervisors and address the previous weakness revealed by the various ML/TF scandals involving certain Estonian and Nordic banks. The Nordic-Baltic cooperation framework consists of representatives from Denmark, Estonia, Finland, Iceland, Latvia, Lithuania and Sweden.

796. According to the EFSA, Estonian FIs usually do not have branches or subsidiaries abroad, but there are branches of foreign FIs in Estonia (five branches as at the end of 2021). The EFSA is host for 5 AML/CFT colleges and part of 10 AML/CFT colleges of other countries. In the Nordic-Baltic cooperation, the Director Generals of the FSAs meet and share information on a yearly basis and on expert level three times a year. The information exchange is about compliance framework of specific entities and cases (including typologies and trends), experience and knowledge. The group also engaged the IMF to conduct regional analysis of ML/TF threats and vulnerabilities. [231]

Table N°8.17: EFSA - Number of outgoing requests for international cooperation

Year	2015	2016	2017	2018	2019	2020	2021
Number of requests sent abroad	6	51	48	58	93	109	102
Number of requests executed by foreign authority	60	51	48	58	93	109	102
Number of requests refused by foreign authority	0	0	0	0	0	0	0

797. When carrying out fit and proper assessments on the owners, beneficial owners, members of the supervisory and management board, as well as on individuals holding significant or controlling interests, who are foreign nationals or have a connection with a foreign jurisdiction,

[230] The full list can be found at the following link: Memoranda of Understanding | FSA (fi.ee)
[231] https://www.fi.ee/en/news/nordic-baltic-countries-engage-imf-conduct-analysis-cross-border-money-laundering-and-terrorist

the EFSA will proactively contact the relevant foreign counterparts (see IO.3). During the period under review, none of the received requests were refused by the EFSA.

798. There is a positive trend in last three years, is the fact that the EFSA has conducted three joint on-site inspections with AML/CFT supervisors from other Member States. These on-site inspections were held together with Member State supervisors, whereas for the two (subsidiaries in Estonia) the decision to initiate a common supervisory action was made together, and for the one (parent company in Estonia), it was the EFSA who proposed to the foreign regulators to start a common supervisory proceeding. The outcome from these joint group level supervisory activities was closer working relationship between the supervisors (see case example below).

Box N°8.3: Group level supervision headed by the EFSA within AML college

In 2020, the EFSA established an AML college for a bank operating in two other EU MS through branches. The college included supervisors from these MS and the EBA as permanent members, with the ECB, the EFSA's Prudential Supervision Division and the EFIU, as observers. During the first meeting of the AML college, the EFSA proposed a joint on-site inspection with the two host supervisors. The joint on-site inspection took place in third quarter of 2020. The supervisors held several virtual meetings before, during and after the inspection to discuss the form and scope of the inspection, analyse findings and to agree on the topics inspected, to coordinate results. The meetings took place on three levels: operational meetings between the onsite teams up to 4 times a month, strategy level meetings between the heads of AML departments and policy level meetings between the heads of supervisors. Based on the extensive cooperation, and mutual input, shortcomings in the institution and its branches, including group level mitigation of risks were identified and remedied. The actions of the supervisors, headed by the EFSA had a positive effect on the group-wide AML/CFT compliance of the credit institution.

Box N°8.4: Joint supervision of a banking group with a subsidiary bank in Estonia

In 2019, the EFSA conducted a joint on-site inspection with the home supervisor of the banking group, which had subsidiary bank in Estonia. The inspections of the parent and subsidiary were conducted separately, but with close cooperation between the EFSA and the home supervisor, including after the on-site inspections.

The exchange of information regarding the inspections and the sanctioning process yielded sanctions and remedial actions taken by both supervisors in a coordinated way ensuring holistic risk management on a group level.

799. The EFSA is also part of several AML Supervisory Colleges where credit institutions operate in Estonia through subsidiaries or branches. The supervisory college is a permanent structure that aims to help college members develop a better understanding of the banks cross-border risk profiles and vulnerabilities with a framework for addressing key issues relevant from a supervisory perspective. The EFSA is part of several colleges with the major banking groups, which is considered as a strength.

The EFIU (as Supervisor)

800. As a supervisor, the EFIU also has the power to seek information from other supervisors regarding DNFBPs, VASPs and some FIs for which the EFIU is responsible for.

801. However, there are no arrangements between the FIU and foreign supervisory authorities for cooperation, including mechanisms and dedicated channels of communication. The EFIU explained that where necessary they would use their FIU-to-FIU channels of cooperation. The AT

considers this not to be an adequate approach, which raises doubts about the capacity of the FIU to seek appropriate international cooperation on the supervisory matters, when needed.

802. The EFIU explained that it is not its practice to seek information from oversees supervisors where applicants or individuals linked to that applicant may be known to those supervisors. There is evidence of some limited communication with overseas banks or central banks where a VASP has banking services provided outside of Estonia, however, these cases appear to be sporadic and exceptional (e.g., about 2% of the total outgoing requests in 2017 and 3% in 2018).

803. There is no evidence that the EFIU has proactive approach in seeking information from foreign supervisors considering their role in supervising sectors which have a more global footprint, particularly CSPs and VASPs. These sectors pose a higher risk for ML and TF, have a strong foreign connection (see IO.3) and so there is considerable merit in proactively contacting supervisors who have assessed applicants and individuals previously, in order to determine or understand if there are matters which would be relevant to the EFIU's assessment of that person.

8.2.4. Providing other forms international cooperation for AML/CFT purposes

The EFIU

804. The EFIU uses all legal powers to provide extensive cooperation to foreign counterparts. When dealing with the foreign requests, the EFIU has mechanism in place enabling timely execution. Authorities explained that there are three main deadlines to be followed when providing cooperation: three days for urgent requests and 14 days if additional analysis should be conducted prior to providing the response. If the case is not marked as urgent, a response is provided within 30 days. The EFIU uses its case management system that allows for prioritisation of incoming requests and can set and monitor the adherence of deadlines. The majority of requests are coming from Latvia, Finland and Lithuania. Starting from 2020 the EFIU analyses its effectiveness of international cooperation, and it can be noted that received feedbacks from international counterparts indicate that responses are timely, useful and of a good quality.[232]

Table N°8.18: EFIU - Number of received requests from different counterparts 2015-2021

Foreign FIU	Number
Latvia	349
Finland	296
Lithuania	233
Russia	178
Germany	197
Ukraine	121
Poland	66
Belarus	59
UK	55
Czech	23

805. Authorities advised that foreign requests are analysed and used as an additional source of information for analysis of domestic cases.

[232] 2020 and 2021 FIU annual overview of international cooperation.

The PBGB

806. The PBGB executes all incoming requests in a timely and effective manner. As explained under core issue 2.3, requests are received through various channels such as INTERPOL I 24/7 and EUROPOL, SIENA. The Estonian SPOC (Single Point of Contact) receives, prioritises, takes actions, and follows up on incoming requests and sends out requests to other authorities. General deadline for executing requests is 30 days, yet urgent requests are supposed to be executed within hours. There is a case management system in place to prioritise the requests and ensure timely execution.

Table N°8.19: PBGB - Number of received foreign ML requests

Year	2015	2016	2017	2018	2019	2020	2021	Total
Number	450	524	573	713	1020	1067	452	**4799**

807. There is increasing number of received requests pertain to ML, as can be seen from the table above. This can be explained by the fact that foreign proceeds are laundered in Estonia.

The ETCB

808. As explained above, the ETCB uses liaisons officers as a way of informal cooperation for the AML/CFT purpose. Officials are strategically posted to jurisdictions deemed high priority for Estonia. However, the exact numbers or case examples have not been provided in order to demonstrate effectiveness.

The EFSA

809. There has been a considerable number of international request received by the EFSA for AML/CTF purposes. Those incoming requests have been executed timely (see table below). The majority of international cooperation with home and host supervisors is coordinated continuously, extensively through the supervisory college platform within college meetings and not using the instrument of separate requests for international cooperation. Some coordinated supervisions took place during the assessment period as explained under previous core issue.

Table N°8.20: EFSA - Number of received AML/CFT requests

Year	2015	2016	2017	2018	2019	2020	2021
Number of requests	2	0	26	26	24	36	39
Executed	2	0	26	26	24	36	39
Refused	0	0	0	0	0	0	0
Average time	30 days	-	30 days	34 days	30 days	31 days	30 days

The EFIU (as Supervisor)

810. As explained under previous core issue, the EFIU does not have arrangements for international cooperation as supervisor, including mechanisms and dedicated channels of communication The EFIU suggested handling and responding to international AML/CFT requests through its core function as a FIU. The AT was not provided with any requests for AML/CFT purposes where the EFIU has been asked to respond only in respect of its supervisory functions rather than its broader AML/CFT function

8.2.5. International exchange of basic and beneficial ownership information of legal persons and arrangements

811. Authorities indicated that the basic and BO information can be exchanged with foreign counterparts. There are basic and BO registers in Estonia, which authorities use when providing assistance to foreign counterparts. However, at the level of companies, OEs, supervisory authorities, investigative authorities and registers it is observed that they do not fully enable availability of adequate, accurate and current BO information in the country. The large share of Estonian companies with e-Residents as their basic or beneficial owners, significant involvement of licensed and non-licensed CSPs in company registration processes, on the background of poorly designed and vaguely understood CDD measures implemented by them are factors with adverse impact on the quality of BO information (see IO.5). This effectively deteriorates the quality of information that Estonia can provide to foreign counterparts.

812. The EFIU advised that BO information is provided as background information in each outgoing request, which concerns legal entities. In order to identify basic and BO information, the EFIU uses BR, internal and some external databases, requests information from the OEs. However, there is no information on the number of received requests for basic and BO information.

813. Regarding the PBGB, the ARO is the competent body to provide and request basic and BO information, but there is no statistics on the number of requests. Different sources of information are used when responding to the requests, such as available registers and databases as well as information held in their own domestic cases.

814. The ETCB does not keep statistics on the number of requests where basic and BO information were requested. However, generally they explained that relevant data is extracted from BR including management board members, shareholders, and BOs, as well as from the legal persons once they are based in Estonia.

815. The EFSA's exchange of BO information with counterparts is a part of the authorisation process and ongoing review of suitability of qualified owners through fit and proper proceedings. The EFSA uses different sources to respond to these requests, e.g., information from LEAs, EFIU, ETCB, and the Consumer Protection Board. The EFSA also uses internal information obtained through AML/CFT supervisory activity and the CR when providing information.

816. There is no information on the number of requests Estonian authorities sent in order to obtain basic and BO information of legal entities in foreign jurisdictions, hence the effectiveness of requesting basic and BO information from foreign counterparts cannot be assessed.

Overall conclusion on IO.2

817. International co-operation is an important component of Estonia's AML/CFT system, given its risk profile and exposure to foreign proceeds being laundered within jurisdiction. Estonia provides and mostly proactively seeks some forms of international cooperation with its neighbouring countries. The Authorities seek international cooperation to large extent regarding predicate offences such as fraud and drug-related crimes. Nevertheless, there is lack of proactivity when seeking assistance to seize and confiscate proceeds of crime moved abroad. Authorities are providing MLA to EU MS and to a somewhat lesser extent to non-EU jurisdictions. There has been a significant number of requests being refused due to the lack of dual criminality and non-

executed. The country's reservation to the Council of Europe Convention on Mutual Legal Assistance in Criminal Matters hinders Estonia's possibility to assist in international cooperation.

818. While the EFSA collaborates closely with its counterparts through supervisory colleges and joint onsite inspections, such cooperation does not exist for the EFIU,

819. Authorities indicated that LEAs, the FSA and the EFIU exchange basic and beneficial ownership information with its counterparts. However, deficiencies identified under IO 5 may hinder the effectiveness of such cooperation.

820. **Estonia is rated as having a Substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2014. This report is available from https://www.coe.int/en/web/moneyval/jurisdictions/estonia.

Recommendation 1 – Assessing risks and applying a risk-based approach

1. The requirements on assessment of risk and application of the risk-based approach were added to the FATF Recommendations with the last revision in 2012 and, therefore, were not assessed during the previous rounds of mutual evaluation of Estonia.

2. ***Criterion 1.1*** – Money Laundering and Terrorist Financing Prevention Act (MLTFPA) provides for the duty to conduct National Risk Assessment (NRA). It should build on relevant information, statistics and analyses, the risk assessments conducted by ministries or agencies in their area of public administration, including the relevant risk assessments, reports and recommendations of international organisations and the European Commission (§11). The most recent nation-wide assessment of money laundering and terrorism financing (ML/TF) risks, an update to the similar assessment covering the period 2011-2013 (hereinafter: the NRA 2015), concerns the period 2017-2019 and has a part with specific analysis for the period 2020-2021 on potential ML/TF risks related to the Covid-19 pandemic (hereinafter: the NRA 2021). The report on the NRA 2021 was endorsed on 28 April 2021.

3. The NRA 2021 methodology considers various factors and scenarios to assess ML/TF threats and vulnerabilities at sectorial and national levels. In the course of conducting the assessment, the authorities identified a number of shortcomings of the methodology and the assessment process, particularly regarding the national threat assessment module, which collected data mainly on predicate offences with little input on important sources of threat (e.g. cross-border movement of funds), contextual factors (e.g. shadow economy, tax gap), contradictory criteria for assessing possible consequences of threats if these were to materialise, etc. Weak and theoretical knowledge of the competent authorities about TF threats was identified as a significant shortcoming in the assessment process. Other issues of organisational and substantial nature, such as the complexity and the duration of the process, which took almost two years, lack of contributions from specific institutions, increased workload of the project members, partial inclusion of representatives from some financial subsectors, and project members missing or leaving certain activities throughout the process were identified, as well. Lack of comprehensive crime statistics, which necessitated manual collection of data, including court decisions on ML crimes, was another significant bottleneck in the conduction of the NRA.

4. In addition to this, the assessment team identified significant shortcomings with the application of the NRA methodology and the outcomes of the assessment. For example, while acknowledging that ML and TF risks are different in nature, and it would be improper to assess them using the same structure and scale of risk factors, the authorities still followed the methodology, including the module of TF threats emanating from predicate offences. At that, the respective working group decided that the threat of TF as a function (weighted average) of

probability and consequence of TF due to all predicate offences was always equal to 1, on a scale of 1-5. First, this raises a question about whether the arithmetic sum of the scores determined for probability and consequences would ever produce the level of threat associated with particular predicate offences, insofar as such sum does not anyhow reflect the causal relationship/ correlation between these two variables. More importantly, the NRA conclusion about the lowest possible level of TF threat (i.e., low probability and very low consequence) in Estonia due to predicate offences, including cybercrime, trafficking of arms and drugs, kidnapping and other serious crimes, is not supported by any analysis and does not amount to a reasonable threat assessment in this area.

5. The assessment team has identified further shortcomings with the application of the NRA methodology regarding all three domains of ML/TF threat, i.e. those pertinent to predicate offences, financial and non-financial sectors, and geographical exposure. The available statistics data does not cover the whole period of the assessment[233]. There is no obvious analytical method for and logical explanation on quantitative and qualitative indicators of threat factors to feed into the determination of probability and consequence ratings within the mentioned domains[234]. The authorities advise that the ratings have been decided by the respective working groups through analysis of available statistics, using their expert knowledge and practical experience in the relevant fields. Nonetheless, the very content of the NRA 2021 report does not provide comprehensive analysis and substantiated judgments to support the above-mentioned ratings, which have been used in the Excel worksheet modules to calculate the scores for threats by means of formulas provided in the methodology.

6. The same, as well as other deficiencies are present regarding input data, assigned ratings and calculated scores for vulnerabilities. For example, ML and TF vulnerability scores calculated for the financial sector (respectively, 2.69 and 2.75), virtual asset service providers (VASPs) (respectively, 4.02 and 3.88), and crowdfunding service providers (respectively, 2.99 and 3.09) lack any analysis and explanation specifying the key determinants that make these sectors exposed to a higher/ lower level of ML vulnerability compared to that of TF vulnerability. A large part of input data on quantitative and qualitative indicators of threats and vulnerabilities in the in the Excel worksheet modules used to calculate the respective scores, which, in turn, underlie calculation of the so-called "risk heat-maps", is not filled in/ is missing.

7. Accordingly, the conclusions of the NRA 2021 report stating that *"the threats and vulnerabilities of the Estonian state as related to money laundering and terrorist financing are at an average level", and that "on a five-point scale, Estonia's money laundering threat level is 2.40, while the nation's terrorist financing threat level is 2.09. Estonian state's money laundering vulnerability level is 2.73, while the terrorist financing vulnerability level is 2.67"*, do not appear to be a reliable assessment of the ML/TF threats and vulnerabilities in the country, both in terms of descriptive estimates and numerical scores. The NRA report, including its Executive Summary, does not set out conclusions on ML/TF risks. As mentioned above, it reflects on threats and vulnerabilities assessed descriptively (high, above average, average, below average, and low) and

[233] E.g. on some threat factors data is available for 2019 only, on others – for 2017-2018, etc.

[234] For example, there is no explanation for rating ML probability of corruption 5 and that of fraud 3, where, in terms of quantitative indicators, the second exceeds the first in terms of the registered crimes, investigations, seized proceeds and, more importantly, the number of ML disseminations made by the FIU, investigations and convictions, as well as the amount of seized, frozen and confiscated proceeds. Likewise, there is no explanation for rating ML consequences of corruption and fraud equally 3.

numerically (on a scale of 1 to 5), which nevertheless do not give a comprehensive view of the (residual) risks of ML and TF in the country.

8. In addition, the Estonian Financial Supervision Authority (EFSA) has conducted ML/TF sectorial risk assessment (SRA) of the financial sector (the supervised sectors). The SRA, mostly covering the period 2014-2020 and endorsed by the EFSA Board on 24 May 2021, i.e. almost simultaneously with the NRA 2021 report. The EFSA has not published the SRA report. The authors of the report advise to have *"proceeded from the World Bank's approach to risk and vulnerability"*. Similarly to the NRA report, the SRA report does not set out conclusions on ML/TF risks, but rather reflects on threats and vulnerabilities in the financial sector descriptively assessed on a 4-level scale (low, medium, high and very high). While not anticipating use of identical methodologies for the NRA and the SRA, the assessment team notes that the differences between these two same-age risk assessment exercises – at least in the way that the findings on identified and assessed constituents of risk are formulated – makes it difficult to conclude on the extent of reconciliation and alignment of their outcomes.

9. For example, the NRA concludes that ML threats are "average" in all subsectors of the financial system, while the SRA sets out that such threats are "moderate" in the subsectors of banks and investment firms and are "low" in the other subsectors. Or, the NRA concludes that the TF threats are "average" for credit and financial institutions (FIs), as well as for providers of payment and currency exchange services, and "low" for insurance and investment firms, whereas the SRA sets out that such threats are "low" in all subsectors. This does not support the authorities' argumentation about different perspectives of the NRA and the SRA allowing more well-rounded understanding of risks. Other shortcomings of the SRA analysis and outcomes are related to the use of contradictory statistical data[235]; circular references to other reports or sources of information[236]; statements not supported by any statistical data or expert judgments[237]; lack of reliable estimates on domestic proceeds of crime and cross-border movements of funds potentially related to ML[238], etc.

10. The Estonian Financial Intelligence Unit (EFIU) has also conducted thematic analyses, such as the 2020 and 2022 surveys on VASPs, the 2021 study of ML risks related to corporate service providers (CSPs), and the 2022 overview of the non-profit sector (NPO). These analyses are a good beginning for identification and assessment of ML/TF risks in the respective sectors, which needs to be further developed in the course of future iterations in order to fill the remaining gaps in the understanding of risk (e.g. the analysis regarding the number of clients, the volume of transactions, as well as internal controls, including risk classification of customers and application of customer due diligence (CDD) measures applied by VASPs is based merely or predominantly on the data presented by service providers, which responded to the EFIU

---

[235] E.g. regarding fraud cases registered in 2019, the SRA refers to 1165 cases in one part of the report, 2191 cases in another, while the NRA data on the same indicator used for calculating exposure to threats from predicate offences refers to 1724 such cases.

[236] E.g. the SRA makes assumptions regarding the amount of proceeds of crime involved in various categories of domestic predicate offenses with reference to *"available statistics and assessments of experts in their respective fields in Estonia"*, while the reports of expert assessments, such as the PBGB Situational Picture of Money Laundering Crimes, refer to the SRA as the original source to provide estimates on proceeds of crimes generated from domestic predicate offences.

[237] E.g. the conclusion stating that *"the Estonian financial environment is unlikely to be used to manage the transit-related cash flows"*.

[238] E.g. the conclusion setting out that *"approximately 120 million euros of funds are generated in Estonia during one year, which could potentially be the object of laundering"*, and the statement summarizing the analysis of cross-border threats reading that *"compared to the domestic threat, the cross-border threats… are significantly larger in value"*.

questionnaire; or, the NPO overview does not specify how exactly the NPOs have been identified as the ones which, by virtue of their activities or characteristics, are likely to be exposed to a higher risk of TF abuse.

11. ***Criterion 1.2*** – According to MLTFPA, the Anti-Money Laundering and Countering the financing of terrorism (AML/CFT) Committee chaired by the Minister of Finance is the government mechanism tasked to coordinate conducting and updating the NRA (§12). This committee formed by a regulation of the Government from 19 April 2018 is comprised of high-level representatives of stakeholder ministries, the EFIU, the EFSA, the Prosecutor's Office, the Estonian Tax and Customs Board (ETCB), the Police and Border Guard Board (PBGB), the Bank of Estonia (BOE) and the Internal Security Service (ISS). It also pursues national cooperation in AML/CFT.

12. ***Criterion 1.3*** – The results of the NRA 2015 covering the period 2011-2013 were endorsed by the AML/CFT Committee on 5 January 2015, followed by the approval of an action plan for 2016-2017. The results of the NRA 2021 covering the period 2017-2019 were endorsed by the AML/CFT Committee on 28 April 2021, followed by the approval of an action plan for 2021-2024. Whereas the law does not establish any periodicity for updating nation-wide risk assessments, it obliges the AML/CFT Committee to keep the NRA up-to-date (MLTFPA § 12 Clause (1)1), and the fact that the first NRA covering the period 2011-2013 was updated not earlier than in 2021 (and that without covering the period 2014-2016) does not enable a conclusion that the requirement of the FATF Standard to keep risk assessments up-to-date is fully met.

13. According to the EFSA AML Rules of Procedure, the SRA is to be updated biennially or at any time when there are new or emerging trends to be taken into account on a sectoral level (Chapter IV, S.4.1). The SRA should also be updated, when the SNRA, the Estonian NRA or the EBA's Opinion on the ML/TF risk affecting the Union's financial sector is updated (Chapter IV, S.4.2). The authorities advise that before the adoption of the first SRA of the EFSA in 2021, sectoral risks were assessed as a part of the RBS model.

14. ***Criterion 1.4*** – The general part of the NRA is published on the Ministry of Finance's (MoF) website (MLTFPA, §11(3)). This is the primary method for the authorities to provide information on the results of risk assessments to self-regulatory bodies (SRBs), FIs and designated non-financial businesses and professions (DNFBPs). The most recent NRA report was published on the MoF website on 25 May 2021, i.e., shortly after its adoption by the AML/CFT Committee. As to relevant competent authorities, the mechanism provided through the AML/CFT Committee enables their participation in and, consequently, awareness of the NRA process and outcomes.

15. The authorities advise that after adoption of the SRA by the EFSA in May 2021, it was introduced to the market through various events since October 2021 (e.g., the AML Public-Private Partnership Forum held on 13 October 2021, the annual information days for all financial sectors held on 7-9 December 2021), as well as communication of the SRA results to the obliged entities (OEs) via letters sent on 4 January 2022. The sectorial analyses conducted by the EFIU are published on its official website[239], while relevant products of the PBGB and the ISS are covered by state secret and thus are introduced to the public sector to a limited extent (e.g., the sections of the ISS yearbooks reflecting on TF aspects).

16. ***Criterion 1.5*** – The AML/CFT Committee prepares an Action Plan for the mitigation of identified risks and designates the authorities that should implement the mitigation measures,

[239] https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#a-survey-of-service-

organises and controls implementation of the action plan within the specified deadlines, develops AML/CFT policies and makes proposals to the respective ministers on the necessary legislative amendments (MLTFPA, §12(1)2, 4)). Action Plans have been developed and endorsed on 30 March 2015 for the period 2016-2017 and on 5 July 2021 for the period 2021-2024. Hence, within the period from 2018-2021 there have been no nation-wide AML/CFT policy to guide risk-based decisions of competent authorities in allocating resources and implementing AML/CFT measures.

17. The authorities advise that the action plans, as endorsed by the AML/CFT Committee, would not necessitate adoption of separate action plans by individual stakeholder agencies. Instead, they feed into the wording of governmental work plans, as well as general or specific work plans of these agencies. Nevertheless, excerpts from the governmental work plans for 2016 and 2019 do not set out actions stemming from the findings of the NRA 2015 and aimed at the application of RBA in allocating resources and implementing measures to prevent or mitigate ML/TF. Moreover, strategies and work-plans of the competent authorities (as much as provided to the assessment team), with some reservation for the 2022 work-plan of the EFIU, do not provide for specific tasks and relevant resources to be channelled to the implementation of the activities defined by the Action Plan developed and endorsed on the basis of the NRA 2021 findings.

18. The EFSA reports significant increase of resources allocated to AML/CFT supervision over the last years, by way of creating a dedicated department since 2019 with 11.2 FTEs as of 2021, along with an additional 5.5 FTEs in supportive (e.g., legal, enforcement, etc.) roles. Over the period 2017-2021, human resources of the EFIU have increased significantly.

19. ***Criterion 1.6*** – According to MLTFPA the following categories of entities are excepted from the AML/CFT framework. Those are: (i) the persons engaged in buying-in or wholesale of precious metals and precious metal articles used for production, scientific or medical purposes; (ii) an insurance undertaking providing services related to mandatory funded pension insurance contracts within the meaning of the Funded Pensions Act; and (iii) a management company upon managing a mandatory pension fund within the meaning of the Funded Pensions Act, and an investment fund founded as a public limited company within the meaning of the Investment Funds Act. Those exceptions are not supported by substantive assessment of ML/TF risks concluding that there is a proven low risk in those sectors or activities, and that those exceptions occur in strictly limited and justified circumstances.

20. ***Criterion 1.7*** – Estonian law provides for both alternatives stipulated under this criterion. The first alternative is: the OE shall apply EDD measures where the risk assessment conducted by the state or by the OE have identified higher ML/TF risks (MLTFPA, §36(3)). The second alternative is: the OE shall base its own risk assessment on the published results of the NRA (MLTFPA, §13(4)).

21. ***Criterion 1.8*** – OEs may apply simplified measures where the risk assessment conducted by the state and by the OE have identified lower ML/TF risks. At that, application of simplified measures is permitted to the extent that the obliged entity ensures sufficient monitoring of transactions, operations and business relationships, so as to enable identification of unusual transactions and notification of suspicious transactions in accordance with the procedure established by MLTFPA. EFSA AML/CFT Guideline further defines that, while conducting their risk assessments and articulating the risk appetite, obliged entities must take into account the

results of risk assessments conducted by supervisory and law enforcement authorities, national and EU risk assessments.

22. ***Criterion 1.9*** – The legislation sets forth requirements for OEs to assess and manage their ML/TF risks, as described under the analysis for c.1.10 and c.1.11 below. Supervision over activities of OEs regarding their compliance with AML/CFT requirements, including those on assessment and management of risks, shall be exercised by appropriate supervisory bodies in accordance with their area of competence (MLTFPA, §64(1-4)).

23. In particular, the EFSA supervises financial institutions[240] except for currency exchange offices and VASPs. All other obliged entities are supervised by the FIU, with the exception of lawyers (attorneys) supervised the BA and notaries supervised by the CN according to the delegation of Minister of Justice. MLTFPA assigns the EFSA, the BA and the CN to cooperate with the FIU for AML/CFT purposes. Reference is made to the analysis for R.26 and R.28 for further details on the structural and substantial elements of the AML/CTF supervisory regime in Estonia. Deficiencies in R.26 and R.28 have bearing on the rating here.

24. ***Criterion 1.10*** – The OEs shall assess their ML/TF risks: identify, analyse and assess such risks associated with their activities (MLTFPA, §13). At the same time, the competent supervisory authorities can decide, at the request of the OE, that "the preparation of a documented risk assessment is not mandatory" for any type of OE or any individual OE (except for the ones supervised by the EFSA) (MLTFPA, §13(5)). The authorities advise that such exemption has been requested only once by auditors and declined by the EFIU.

25. *a) Document risk assessments* –Risk assessments conducted by OEs should be documented (MLTFPA, §13(4)).

26. *b) Consider all relevant risk factors* –OEs shall take into account at least the risks relating to: i) customers; ii) countries, geographic areas or jurisdictions; iii) products, services or transactions; and iv) communication, mediation or products, services, transactions or delivery channels between the OE and the customers (MLTFPA, §13(1)).

27. *c) Keep assessments up to date* – The risk assessment conducted by the OE should be documented and updated where necessary and based on the published results of the NRA (MLTFPA, §13(4)).

28. *d) Have mechanism for providing risk information to authorities* – At the request of the supervisory authority OEs should submit to them the documents related to their risk assessments (MLTFPA, §13(4)). This covers the BA and the CN, which are the supervisors for, respectively, lawyers (attorneys) and notaries (MLTFPA, §64).

29. ***Criterion 1.11*** – The OEs shall establish rules of procedure that allow for effective mitigation and management of ML/TF risks as per the conducted risk assessments (MLTFPA, §13-14). To this end, OEs should define internal control rules that describe the internal control system, including the internal audit function and, where necessary, compliance control. The competent supervisory authorities may grant, at the request of the obliged entity, "partial or full release from the obligation to prepare documented rules of procedure and internal control rules" to any type

[240] In particular, credit institutions, life insurance companies, securities firms, fund management companies, PSPs, e-money institutions and consumer credit loan providers, as well as branches of the said institutions operating in Estonia through the freedom of establishment principles.

of reporting entities or any individual reporting entity (except for credit and financial institutions), the authorities advise that such exemption has never been granted.

30. *a) Have policies, controls and procedures* –The rules of procedure and the internal control rules, which may be contained in a single document or in multiple documents, must be proportionate to the nature, size and level of complexity of the OE's activities and should be established by its senior management (MLTFPA, §14(3)).

31. *b) Monitor implementation of controls* –The OEs shall adhere and implement the rules of procedure and internal control rules by the employees, to check regularly whether these rules are up to date and, where needed, establish new ones or make necessary modifications into them, as well as to make adherence to them subject to checks by the internal audit (where the OE has one) (MLTFRA, §14(2-5)).

32. *c) Take enhanced measures* – Reference is made to the analysis for c.1.7 (with regard to FIs and DNFBPs) and c.10.17 (with regard to FIs) on the requirement to take enhanced measures to manage and mitigate higher risks where identified.

33. ***Criterion 1.12*** – Reference is made to the analysis for c.1.8 and c.10.18 on the application of simplified measures, for c.1.9 on the supervision to ensure implementation of obligations under R.1, as well as for c.1.10 and c.1.11 on the implementation of risk assessment and mitigation measures by OEs.

Weighting and Conclusion

34. Estonia made efforts to assess and analyse its ML/TF risks through two NRAs and a number of sectoral risk assessments, which together contributed to countries risk understanding. Nevertheless, gaps remain. The following are considered to have a heavier weight in determining the rating for this Recommendation: there are significant shortcomings with the application of the country-wide risk assessment methodology and the outcomes of the assessment; other strategic analyses need to be further developed in order to fill the gaps in the understanding of risk (c.1.1); nation-wide policies to guide risk-based decisions have not been available for the whole period under consideration and are not reflected in strategies and work-plans of the competent authorities (c.1.5); exceptions from the AML/CFT framework are not supported by substantive assessment of ML/TF risks (c.1.6). **R.1 is rated Partially Compliant (PC)**

Recommendation 2 – National Cooperation and Coordination

35. In the 4th round MER of 2014, Estonia was rated largely compliant (LC) with former Recommendation (R.) 31. The assessment concluded that there was insufficient cooperation and coordination between supervisory authorities.

36. ***Criterion 2.1*** – MLTFPA (§11) defines that NRAs identify the needs for drafting and amending AML/CFT legislation, as well as other regulations and guidelines in the area; guide the competent authorities regarding allocation of resources and setting of priorities for AML/CFT purposes; and reflect on the institutional structure and general procedures of the AML/CFT regime. Accordingly, the action plans developed and endorsed on 30 March 2015 and 5 July 2021 building on the outcomes of the first and second NRAs are considered as the key national

AML/CFT policies in the country informed by risk assessments and updated on regular basis (MLTFPA, §12).

37. ***Criterion 2.2*** – The AML/CFT Committee is the national body of executive power that, *inter alia*, develops AML/CFT policies, including the action plan for the mitigation of identified risks and designates the authorities that should implement the mitigation measures, organises and controls implementation of the action plan within the specified deadlines (MLTFPA, §12).

38. ***Criterion 2.3*** – All policy makers, including the EFIU, LEAs, supervisors (excluding SRBs) and other relevant competent authorities are represented in the AML/CFT Committee (see also the analysis for c.1.2). The committee is well-positioned to provide domestic coordination and exchange information concerning the development and implementation of AML/CFT policies and activities at policymaking level.

39. The authorities advise that, for coordination purposes with the private sector, the AML/CFT Committee has established on 2 May 2018 an advisory committee of the representatives of OEs (the Market Participants Advisory Committee). In addition, five other ad hoc and standing working groups[241] have been established to facilitate implementation of strategic and operational tasks. All these working groups are run by the MoF, except for the Operational Working Group run by the EFIU.

40. As another method to facilitate domestic cooperation and coordination, the authorities refer to the common practice of concluding bilateral MOUs between competent authorities such as the EFIU, the PBGB[242], the PO, the ETCB, the EFSA, etc. The EFIU has also signed MOUs with the CN and the BA, which currently are in the process of renewal.

41. ***Criterion 2.4*** – The AML/CFT Committee shall pursue, *inter alia*, national cooperation in countering proliferation (MLTFPA, §12), but not the financing of proliferation, and it is not clear what specific tasks are performed by the committee towards realisation of this mandate. In terms of institutional arrangements, CPF is considered in the context of the International Sanctions Act (§9(21)), which defines the MFA as the lead agency in coordinating national implementation of international sanctions. The secretary general of the MFA is also a member of the AML/CFT Committee. Two commissions within the MFA, i.e., the Strategic Goods Commission (SGC)[243] and the Sanctions Commission provide platforms for coordination and information exchange in CPF matters. The coordinator of the SGC participates on a regular basis in AML/CFT Committee meetings and gives an overview on matters related to implementation of, *inter alia*, the UNSCR 1540 on the prohibition of weapons of mass destruction, as well as on measures to control export of dual-use and military goods.

42. ***Criterion 2.5*** – The Data Protection Inspectorate (DPI), which is a governmental agency under the Ministry of Justice (MoJ), is involved in the legislative procedure, as well as in the development of policies, strategies and development plans related to its field of activity pursuant

---

[241] These include the Working Group of Experts on the Institutional Framework for Combating ML/TF (ad hoc working group established on 02 November 2018); the Working Group of Experts on the Procedural Framework for the prevention and sanctioning of ML/TF (ad hoc working group established on 18 March 2019); the Working Group of Communication Experts on Combating ML/TF (permanent/standing working group established on 18 March 2019); the National Risk Assessment Steering Committee (ad hoc working group established on 30 April 2019); and the Working Group of Experts at the Operational Level of Combating ML/TF (permanent/standing working group established on 16 June 2021).

[242] In the person of its Economic Crimes Bureau, which is part of the National Criminal Police.

[243] The commission consists of the representatives from the PBGB, the TCB, the ISS, MD and the MEAC; it issues licenses to registered brokers of military goods under the International Sanctions Act.

to the Government regulation "Rules for Good Legislative Practice and Legislative Drafting" (§50). This regulation sets the requirement to consult, collect and consider the opinions of competent state authorities.

43. The authorities advise that the DPI has been engaged in the drafting process of MLTFPA and the respective by-laws. Due to this, references to the data protection and privacy rules have been added into the relevant provisions of the MLTFPA (e.g., §14 on the rules of procedure and the internal control rules, §20 on due diligence measures, §48 on the rules regarding data protection in implementing AML/CFT requirements). The DPI exercises supervision over the legality of the processing of information maintained in the EFIU (MLTFPA, §69).

Weighting and Conclusion

44. **R.2 is rated Compliant (C).**

Recommendation 3 – Money laundering offence

45. In the 4th round MER of 2014, Estonia was rated LC on former R.1. There was a technical deficiency in that the purposive requirements extended to the offence of acquisition, use and possession, thus narrowing the scope of the offence in self-laundering cases, and that TF was not fully covered as a predicate offence for ML.

46. ***Criterion 3.1*** – In Estonia, ML is criminalised by Penal Code (§ 394), with ML being defined in the MLTFPA. The definition incorporates the elements from Article 6(1) of the Palermo Convention and Article 3(1) (b) & (c) of the Vienna Convention. The offence includes (i) conversion or transfer of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions; (ii) the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein; (iii) the concealment of the true nature, origin, location, manner of disposal, relocation or right of ownership of property acquired as a result of a criminal activity or property acquired instead of such property or the concealment of other rights related to such property. Although there is no clear reference in either of the two laws that this definition is authoritative for the purposes of the Penal Code where the criminal sanctions for the ML offence are prescribed, in practice, Estonian criminal courts refer to this definition in their judgements.

47. ***Criterion 3.2*** – Criminalisation of ML covers laundering of property derived from "criminal activity" and therefore adopts an "all crimes" approach to predicate offences. This encompasses the full range of offences in 21 categories of designated predicate offences and more. Nevertheless, there remain some gaps in criminalisation of TF, impacting the range of offences that should be covered.

48. ***Criterion 3.3*** – This criterion is not applicable because all criminal offences may be predicate offences for ML.

49. ***Criterion 3.4*** – Property is defined as "any object, as well as the right of ownership of such object or a document certifying the rights related to the object, including an electronic document, and the benefit received from such object" (MLTFPA, §3). In addition, the General Part of the Civil Code (§48) and jurisprudence has confirmed that this definition is wide and covers all property as required by the standards.

50. ***Criterion 3.5*** – Incrimination of ML offence does not require conviction for predicate offence to prove that property is the proceeds of crime (MLTFPA, §4 (5)).

51. ***Criterion 3.6*** – The ML offence extends to the proceeds of criminal activity carried out in the territory of another country (MLTFPA, §4(3)).

52. ***Criterion 3.7*** – The ML offence does not differentiate between laundering the proceeds of a person's own offences or the offences of a third party and hence, it does not preclude self-laundering as an offence (MLTFPA, §4).

53. ***Criterion 3.8*** – The knowledge, intention or purpose which are required as elements of the ML offences may be inferred from objective factual circumstances (MLTFPA, §4(4)).

54. ***Criterion 3.9*** – The sanctions for natural persons for ML offence can be considered proportionate but not fully dissuasive.

55. ML offence is punishable, for natural persons, by a pecuniary punishment or up to a maximum of five years' imprisonment. In addition, imprisonment sanction increases whereby the ML is (i) committed by a group (ii) done at least twice (iii) on a large-scale basis or (iv) if committed in the course of the economic or professional activities of the obligated person. In such circumstances, there is no pecuniary punishment available, but the minimum imprisonment is two years, and the maximum ten years. Conclusion of an agreement for the purpose of execution of ML is punishable by pecuniary punishment or a maximum of two years of imprisonment. The maximum pecuniary punishment is 500 "daily rates" (Penal Code §44). A daily rate for natural person is calculated based on the average daily income of the offender and the minimum daily rate in such case is 10 Euros. Comparing sanctions' range for ML with other serious criminal offences (such as drug trafficking) it is evident that envisaged sanctions are not fully dissuasive. Nevertheless, those deficiencies are minor.

56. ***Criterion 3.10*** – Legal person can be held liable for ML offence (Penal Code § 394). There is no obstacle to parallel criminal, civil, or administrative proceedings with respect to legal persons. The financial sanctions for legal persons are proportionate and dissuasive. Legal person can be punished for ML offence by fine. Maximum pecuniary punishment is set to 500 "daily rates." (Penal Code § 44). A daily rate is calculated based on the average daily income of the annual turnover of the legal person during the financial year. For legal persons the range of pecuniary punishments is from EUR 4 000 to EUR 16 000 000.

57. ***Criterion 3.11*** – The ancillary ML offences (including participation in, association with, or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission) are criminalised (Penal Code, § 22, 22.1, 25 §394.1). Furthermore, the MLTFPA (§ 4(2)) confirms that "Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the activities referred to in (§ 4(1))."

Weighting and Conclusion

10. Estonia covers majority of elements required by the recommendation. However, minor deficiencies are identified with respect to the range of criminalised predicate offences as described under R.5, as well as sanctions for ML offence. Therefore, **R.3 is rated LC.**

Recommendation 4 – Confiscation and provisional measures

58. In the 4th round MER of 2014, Estonia was rated PC on former R.3. The technical issues identified were with regard to confiscation and seizure of property of corresponding value of instrumentalities and laundered property, confiscation when owner or possessor not identified, confiscation as regards property intended for TF, and deficiency with the criminalisation of TF. In July 2019, the MONEYVAL Plenary concluded that Estonia had addressed majority of the deficiencies identified in the 4th MER.

59. ***Criterion 4.1*** – The Penal Code provides Estonia's framework for confiscation.

60. a) *Property Laundered*: In Estonia, laundered property in instances when ML is prosecuted as a standalone offence is considered as direct object of ML offence and can be confiscated (Penal Code, §394(5) and §83(2)). However, if ML offence is prosecuted together with predicate crime, laundered property will be considered as proceeds of predicate crime and shall be confiscated (Penal Code, §83^1(1)).

61. b) *Proceeds, including income or other benefits derived from proceeds, and instrumentalities used in or intended for use in ML or predicate offences:* In Estonia, proceeds of any crime, shall be confiscated if they belong to the offender at the time of issuing the judgment or ruling (Penal Code § 83^1). This includes confiscation of incomes or other benefits deriving from the proceeds (Penal Code, §83^1(2)). In addition, if proceeds of crime belong to third person at the time of judgement, confiscation shall be ordered against third person, respecting the rule of *bona fide* third party.

62. Instrumentalities may be confiscated if (1) an object which was used or intended to be used to commit an intentional offence and (2) the substance or object which was the direct object of the commission of an intentional offence, or the substance or object used for preparation of the offence (Penal Code § 83). The confiscation of instrumentalities can apply if the objects belong to the offender at the time of the making of the judgement or ruling (Penal Code, §83(1) and (2)). Where objects or substance belongs to third parties, discretional confiscation is possible only if the person (i) recklessly or otherwise aided the use of the objects for the offending, (ii) has received the property as a gift or for a price considerably lower than market value, or (iii) has knowledge that the property is transferred to them to avoid confiscation (Penal Code, §83(3)).

63. c) *Property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations*: General provision of the Penal Code dealing with the confiscation of instrumentalities and proceeds of crime (§ 83 and 83.1) is also applicable to property that is proceeds of, or used in, or intended or allocated for use in terrorism related offences. Confiscation is also discretionary, and the property must belong to the offender at the time of judgement.

64. d) *Property of corresponding value:* In case proceeds of crime, assets acquired by a criminal offence or instrument by which a criminal offence was committed, or direct object of a criminal offence have been transferred, consumed or the confiscation thereof is impossible or unreasonable for another reason, the court may order payment of an amount which corresponds to the value of the assets subject to confiscation (Penal Code, §84).

65. ***Criterion 4.2 –*** Estonia has measures in place to allow competent authorities to:

66. a) *Identify, trace and evaluate*: In the course of investigation of criminal offence the LEAs are empowered to conduct financial investigations in order to identify, trace and evaluate the property. When identifying and tracing proceeds LEAs can interrogate witnesses (CCP, §68),

inspection of documents (CCP, §86), search (CCP, §91) and conduct surveillance measures (CCP, §126.2 and §126.3). Banking secrecy shall not represent obstacle to obtain information once the criminal investigation is initiated. Regarding evaluation of property, the expert or specialist witness who participated in the procedural operation ascertains the value of the property (CPC, §142(6)).

67. b) *Provisional measures*: There are provisions enabling preservation of property that may be subject to confiscation (CPC, §142). Assets are seized at the request of the PO based on an order of a preliminary investigation judge or based on a court order. The PO, in cases of urgency, can order seizure of assets summarily but a preliminary investigation judge must be informed within 24 hours and he or she can grant or refuse the seizure (CPC, §142(12)). Once ordered, seizure measures are disclosed to the person whose property is concerned (CPC, §142(5)). This means that initially the application of seizure of property subject to confiscation may be made *ex-parte* or without prior notice.

68. c) *Preventing or voiding actions*: In Estonia, based on the Civil Code (§88(1)) any action aimed to dispose assets restrained by court order is void.

69. d*) Appropriate investigative measures*: Authorities can take investigative measures as set out in R.31.

70. ***Criterion 4.3 –*** Bona fide third party are exempted from confiscation (Penal Code, §85(2)). They can take certain procedural steps (CCP, §40.1 and §40.2), and can participate in judicial proceedings, enjoying all the rights of participants in proceedings as provided for in the Code (CCP, §17). Finally, confiscation shall not be applied to assets of a third party which have been acquired 5 years (2nd degree offence) or 10 years (1st degree offence) earlier, before the commission of the criminal offence (Penal Code, §83.2(3)).

71. ***Criterion 4.4 –*** Estonia has in place mechanisms for managing and disposing of seized and confiscated property (CCP, § 125 - storage of physical evidence and CCP, §126 -measures applicable to physical evidence and confiscated property). Property is managed by the Logistics Bureau of the Police and Border Guard Board, with several regulations, authorisations and directives governing the procedure for asset management.

Weighting and Conclusion

72. **R.4 is rated C.**

Recommendation 5 – Terrorist financing offence

73. In the 4th round MER of 2014, Estonia was rated PC on former SRII. The Estonian authorities were recommended to introduce to §237 of the Penal Code the criterion that the collection of funds with the intention that they should be used, or in the knowledge that they are to be used by an individual terrorist for any purpose rather than terrorist purposes and criminalise the indirect provision or collection of funds. Furthermore, Estonian was recommended criminalise all the financing of all conducts referred to in Article 2.1(a) of the TF Convention. Estonia was also recommended to remove the additional purposive element provided under §237 of the Penal Code; "if committed with the purpose to force the state or an international organisation to perform an act or omission […]".

74. ***Criterion 5.1*** – Estonia criminalises TF offence (Penal Code, §237.3) as "financing or knowingly supporting in another manner commission of acts of terrorism (Penal Code, §237(1)), terrorist organisations (Penal Code, §237.1), preparations of and incitements to acts of terrorism

(Penal Code, §237.2). The offence also covers provision or collection of funds to terrorist organisations or individuals whose activities are directed to commission of criminal offence of terrorism, as well as making available or accumulating of funds while knowing that these may be used in full or in part to commit a criminal offence provided for in §237, 237.1 or 237.2 of the Penal Code. Authorities advised that direct and indirect collecting and providing funds are covered in criminalisation of TF offence (supporting in another manner).

75. Estonia did not ratify the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation. In addition, some acts which constitute an offence in other Conventions listed in the Annex of the TF Convention[244] appear not to be fully criminalised, and overall financing of all acts from UN terrorist conventions does not constitute an offence.

76. ***Criterion 5.2*** – TF offence extends to financing or knowingly supporting in another manner (i) commission of terrorist act (ii) terrorist organisation or a person whose activities are directed at commission of a criminal offence of act of terrorism. There is no need to establish link to specific terrorist act (Penal Code, §237.3).

77. ***Criterion 5.2bis*** – Penal Code (§ 237.5) criminalises travel to another state for the purpose to commit a criminal offence established in § 237 and 237.1, or for the purposes or organisation or receiving training provided for the offence in §237.2. Furthermore, §237.6 of Penal Code, criminalises organisation, preparation (In Estonian *„ettevalmistamine"* which includes planning) funding or knowing support in another manner of a criminal offence from §237.5 and making available or accumulation of funds while knowing that these may be used in full or in part to commit a criminal offence provided for in §237.5.

78. ***Criterion 5.3 –*** The wording of the TF offence does not use the term funds. However, it can be concluded that "financing or supporting in another manner" is broad enough to cover any funds or other assets whether from a legitimate or illegitimate source. Estonia does not require that the funds or other assets were used to carry out or attempt a terrorist act (Penal Code, §237.3). This interpretation of the law was confirmed by jurisprudence[245].

79. ***Criterion 5.4*** – Incrimination of TF offence in Estonia does not require that the funds or other assets were used to committee TF offence neither there should be link to specific terrorist offence.

80. ***Criterion 5.5*** – In Estonia there is no legal provision enabling intent and knowledge required to prove the offence to be inferred from objective factual circumstances. However, authorities indicated that when assessing intent in every case all relevant evidence will be taken into consideration including objective factual circumstances.

---

[244] Offences listed in the Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988 and Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988 are not fully covered in the Estonian Penal Code.

[245] Supreme Court Judgement 3-1-1-100-16; April 10th, 2017, para.15 "…it follows that if a person is convicted under first alternative comprising the necessary elements of an offence of s.237[1] (1)of Penal Code…..it must be verified, in addition to the act of financing or supporting which offence provided for in s. 237, 237[1] or 237[2] of Penal Code the act of financing or supporting was directed towards to facilitate. Whether or not the offence or attempted offence provided for in s. 237, 2371 or 2372 of Penal Code is or is not committed is irrelevant to the prosecution of the supporter…."

81. ***Criterion 5.6*** – Persons convicted for TF offence can be sentences between 2 and 10 years of imprisonment. These sentencings appear to be proportionate to other terrorism related crimes and dissuasive.

82. ***Criterion 5.7*** – In Estonia, a legal person can be held liable for TF offence (Penal Code, § 237.3(2)). Furthermore, general party of Penal Code defines liability of a legal person for an act committed in the interests of the legal person by its body, a member thereof or by a senior officer or competent representative (Penal Code, §14). The liability of legal person does not prevent liability of natural person. The offence is subject to fines between EUR 4 000 and 16 000 000 (Penal Code, §44(8)).

83. ***Criterion 5.8*** – (a) Attempted TF is criminalised through §25 of Penal Code.

(b) Accomplice is criminalised through §22 of Penal Code and covers abetting and aiding.

(c) Organising or directing others is covered by the provisions of an accomplice in §22(2) of Penal Code.

(d) Contribution is covered by the provision of aider in §22(3) of Penal Code.

84. ***Criterion 5.9*** – Due to the all-crimes approach applied in Estonia the TF offence is a predicate offence for ML.

85. ***Criterion 5.10*** – Estonian Penal Code does not make any distinctions regarding the place where the terrorist or terrorist organisation is located, or the terrorist act occurred or will occur. If the terrorist(s)/terrorist organisation(s) is located in another country or the terrorist act(s) occurred or will occur in another country and the person alleged to have committed the financing of these persons or these acts is in Estonia the TF offence appears to be applicable. There does not appear to be anything in the legislation which limits the TF offences in contravention of this criterion (Penal Code, §7 and §8)

Weighting and Conclusion

86. In Estonia, definition of TF offence does not meet all criteria required under R.5. Even though majority of offences listed in the Annex of TF Convention are criminalised, their financing is not considered to be a TF offence. **R.5 is rated LC.**

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

87. In the 4th round MER of 2014, Estonia was rated PC on former SR.III. Identified shortcomings were: (i) absence of a requirement to apply freezing measures under UNSCR 1267 and 1373 without delay; (ii) absence of obligation for the purposes of UNSCR 1267 to freeze funds derived from funds or other assets owned or controlled, directly or indirectly by persons or entities included in the UN list or by persons acting on their behalf or at their direction; (iii) lack of measures taken to freeze funds of persons formerly known as "EU internals"; (iv) absence of a legislative framework to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions; (v) lack of clear publicly-known procedures for unfreezing in a timely manner funds and assets.

88. Estonia implements UNSCRs through the domestic legislation ISA and the EU legislation. As concerns the EU legislative framework, UNSCR 1267/1989 (on Al Qaida) are implemented through the EU Council Decision 2016/1693/CFSP and EC Regulation 881/2002; UNSCR 1988 (on Taliban) – through EU Council Decision 2011/486/CFSP and EC Regulation 753/2011; and

the UNSCR 1373 - through EU Council Common Position (CP) 2001/931/CFSP and EC Regulation 2580/2001. The EC Regulations have direct legal effect in Estonia as per general EU law principles.

89. ***Criterion 6.1*** – (a) In Estonia, the authority responsible for proposing persons or entities to the UN Committees 1267/1989 and 1988 is the Ministry of Foreign Affairs (MFA). (International Sanctions Act (ISA), §8.1(1)).

90. (b) In Estonia, there are formal procedures establishing the process for identification of targets for designations based on the designation criteria set out in the UNSCRs (ISA, §8.1(3)) and the "Guidelines for Proposing the Designation or Removal of a Natural or Legal Person, Entity or Body from the List of Subjects of an International Sanction" adopted by the Government Order on 17 March 2022 (ISA Guidelines)).

91. (c) At the time of making the proposal for designation there has to be reasonable doubt that the natural or legal person, entity or body contained in the proposal meets the criteria for designation under the respective UNSCRs. The initiation of criminal proceedings against a natural or legal person, entity or body identified in the proposal shall not be a precondition for designation (ISA Guidelines, point 2(4-5)).

92. (d) The MFA shall submit a proposal for designation to the UN Committees 1267/1989 or 1988 in the format established by that Committees (ISA Guidelines, point 2(6)). The Guidelines do not specify that the authorities will follow the procedures established by that Committees.

93. (e) When making a proposal, Estonia shall collect, consider and submit all the relevant information as required by the respective UNSCR (ISA Guidelines, point 1(3)). The legislation does not stipulate that Estonia shall specify whether its status as a designating state may be made known.

94. ***Criterion 6.2*** **–** In relation to designations pursuant to UNSCR 1373 Estonia implements those through the EU and national mechanisms:

95. (a) *At the EU level*, the EU Council (through the Council's Working Party on the Application of Specific Measures to Combat Terrorism (COMET WP)) is the competent authority for making designations according to CP 2001/931/CFSP (Art.1(4)) and EC Regulation 2580/2001 (Art.2(3)). These do not include persons, groups and entities having their 'roots, main activities and objectives with the EU (EU internals).

96. *At the national level* the Government of Estonia is the competent authority for imposing sanctions by regulations, followed by the designation of persons and entities by a Minister of MFA. This is done upon the proposal of the MFA (ISA, §4 and §27(1-2)). On the own motion, or when a foreign country request is received the ISS shall assess the request against the criteria for designation as per respective UNSCRs and provide this information to the MFA for further actions (ISA Guidelines, points 1(5) and 2(1-2, 7)). The national legislation allows for listing the EU internals.

97. (b) *At the EU level*, the competent authority of the EU Member State submits a proposal for listing (the MFA for Estonia). The COMET WP prepares and makes recommendations for

designations. The EU Council applies designation criteria set in the CP 2001/931/CFSP (Art.1(2) and (4)), and EC Regulation 2580/2001(Art.2(3)).

98. *At the national level,* the mechanism for identifying targets for designation based on the designation criteria set out in UNSCR 1373 is established by the ISA Guidelines (points 1-2).

99. (c) *At the EU level*, requests for designations are received and examined by the COMET WP, which evaluates and verifies information, including the reasonable basis for request, to determine whether it meets the criteria set forth in UNSCR 1373. No clear time limit has been set for the procedural steps to accomplish before the COMET WP circulates the proposal to delegations. Once circulated, delegations are given 15 days, which in exceptional instances can be further shortened (doc. 14612/1/16 REV 1 on establishment of COMET WP, ANNEX II Art. 9-10).

100. *At the national level,* when a foreign country request is received the ISS shall immediately assess the request and the provided information against the criteria of the respective UNSCRs (ISA Guidelines, points 1, 5).

101. (d) *At the EU level*, the COMET WP assesses and evaluates whether the information for designation meets the criteria set out in CP 2001/931/CFSP. Designation decision shall be based on serious credible evidence without condition upon the existence of an investigation or conviction (CP 2001/931/CFSP, Art.1(2) and (4)).

102. *At the national level,* at the time of making the proposal for designation there has to be reasonable doubt that the natural or legal person, entity or body contained in the proposal meets the criteria for designation under the UNSCR. The initiation of criminal proceedings against a natural or legal person, entity or body identified in the proposal shall not be a precondition for making the proposal for designation (ISA Guidelines, point 2(4-5)).

103. (e) *At the EU level,* there is no specific mechanism that would allow for requesting non-EU member states to implement the EU restrictive measures. Within the scope of the approximation procedure countries aspiring to join the EU are proposed to be invited to align themselves with the EU Council Decisions.

104. *At the national level*, there is no formalised procedure under which Estonia would request another country to give effect to freezing measures undertaken by competent authorities. Nevertheless, where would need to do so, this will be done through the MFA, within the scope of implementation of foreign policy matters. The MFA will use the diplomatic channels of communication and provide information and supporting evidence to foreign competent authorities when requesting another country to give effect to domestic freezing actions (Statute of the MFA, §8(1) and Foreign Relations Act, §9(1(1)).

105. ***Criterion 6.3*** – (a) *At the EU level*, the Member States shall provide the widest possible assistance in countering terrorism, through police and judicial co-operation in criminal matters (CP 2001/931/CFSP (Art.4)). The Member States are required to communicate all relevant information available to them under the EU Regulations on TFS (EC Regulation 2580/2001 (Art.8), EC Regulation 881/2002 (Art.8), and EC Regulation 753/2011 (Art.9)).

106. *At the national level* when the Estonian authorities receive information which could give rise to the designation of a person or entity pursuant to UNSCRs, they shall notify the ISS, which is empowered to collect and solicit information from EFIU, LEAs the GPO and courts, as well as from the relevant foreign authorities in order to verify and establish whether the criteria for

designation per respective UNSCRs are met (Security Authorities Act, §21.1, §32 and the ISA Guidelines, points 1 and 4).

107. (b) *At the EU level*, as for the UNSCRs 1267/1989 regime, the Council Decision 2016/1693/CFSP (Art.5(2) and (3)) and EC Regulation 881/2002 (Art.7a) provides for *ex parte* proceedings against a person or entity whose designation is considered. The Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the designation. Other respective regulatory measures[246] are silent on application of measures *ex parte*.

108. *At the national level*, operation *ex parte* against a person or entity when identified or designated is ensured by the provisions of ISA that specify that the Administrative Procedure Act shall not apply to the designation of the subjects (§27(3)).

109. ***Criterion 6.4 –*** *At the EU level,* implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not yet occur "without delay." There is often a delay between the date of the UN designation and its transposition into the EU law. For resolution 1373, TFS are implemented without delay because, once the decision to freeze has been taken, EU Regulation 2580/2001 is immediately applicable within all EU Member States.

110. *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 respective UN Committee established on the basis of the resolution until the regulation of the EU Council 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.

111. ***Criterion 6.5 –*** In Estonia, the MFA is a coordinating body for implementation of the international sanctions (ISA, §10(1)). The EFIU is a designated authority for implementation and enforcement of the TFS under the Estonian national legislation (ISA, §11(3)3)). The EFSA exercises supervision over compliance of application of financial sanctions by its supervised OEs (ISA, §30(1.1)). The BA and the MoJ (or when delegated - the Chamber of Notaries (CN)) carry out supervision of lawyers and notaries (ISA, §30(4),(5)).

112. (a) *At the EU level,* in relation to UNSCRs 1267/1989 and 1988, EU Regulations establish the obligation to freeze all the funds and economic resources belonging to a person or entity designated on the European list (EC Regulation 753/2011 (Art.3 and 14) and EC Regulation 881/2002 (Art.2(1) and 11).

113. For UNSCR 1373, the obligation for natural and legal persons to freeze the assets of designated persons derives automatically from the entry into force of the EU Regulation, without any delay and without notice to the designated individuals and entities (EC Regulation 2580/2001 (Art.2(1a) and 10). Listed EU "internals" are not subject to freezing measures but only to increased police and judicial cooperation among members (CP 2001/931/CFSP footnote 1 of Annex 1).

114. *At the national level*, natural and legal persons are obliged to apply financial sanctions. Financial sanctions are referred to as the international sanctions that establish freezing obligation (ISA, §14(1)), hence extend to the UNSCRs 1267/1989 and 1988, and include the measures taken within the scope of UNSCR 1373. Those financial sanctions should be applied in the circumstance

[246] Council Decision 2011/486/CFSP and EC Regulation 753/2011; CP 2001/931/CFSP.

when the natural or legal person establishes or has doubts that a person who has or is planning to have a business relationship with them is a designated person or entity, or a transaction or act intended or carried out by that person or entity violates financial sanctions (ISA, §19). This provision limits the freezing obligations respectively to specific circumstances only.

115. At the same time, the ISA sets out obligation for implementation of financial sanctions specifically by "persons having specific obligations" and "legal service providers" (§20-21 and 24). The coverage of those specified entities does not extend to (i) types of FIs and DNFBPs that are not covered under the AML/CFT requirements (see also R.1(c.1.6)); and the DNFBPs, except for the legal service providers. Thus, all those non-covered entities would be captured under the obligations set forth for all natural and legal persons, as above. In addition, implementation of financial sanctions by the persons having specific obligations is limited to circumstances when the designated person has or is planning to have a business relationship with them or that the transaction or act intended or carried out by a designated person is in breach of financial sanctions. As concerns the legal service providers (notaries, lawyers and others) their obligation for implementation of financial sanctions is limited to representation of a client when conducting specified list of operations only.

116. (b) *At the EU level*, freezing obligations extend to all funds and economic resources, including interest, dividends or other income on or value accruing from or generated by assets belonging to, owned, held or controlled directly or indirectly by the designated person or entity or a third party acting on their behalf or at their direction. This is ensured for UNSCR 1267/1989 through EU Regulation 881/2002 (Art. 1(1) and 2(1)), and for UNSCR 1988 – cumulatively through the provisions of Council Decision 2011/486/CFSP (Art.4(1)) and EC Regulation 753/2011 (Art.1(a) and Art.3(1)). There is no explicit reference to assets owned jointly.

117. With regard to UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EU Regulation 2580/2001, Art. 2(1(a)). There is no explicit reference to the freezing of funds or other assets controlled by, indirectly or jointly owned by, or derived from assets owned by, or owned by a person acting on behalf of, or at the direction of a designated person or entity. However, this gap is largely mitigated by the EC's ability to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, Art.2(3) (iii) and (iv)).

118. While the gap related to the absence of provisions on the assets jointly owned, as identified in all three instances remains, the non-binding EU Best practices for the implementation of restrictive measures (8519/18, para. 34) and EU Council Sanctions Guidelines (para. 55a) clarify this matter.

119. *At the national level*, the obligation to freeze extends to funds and economic resources of a designated person (ISA, §5, §14(1), §19 and §21(1)), including when those are owned jointly (§15(1)). However, domestic legal provisions do not cover the requirement to freeze funds and other financial assets or economic resources of the entities owned or controlled indirectly, by designated persons or entities, those derived or generated from funds or other assets owned and controlled by the designated persons and entities, as well as funds or other financial persons and entities acting on their behalf, or at the direction of, designated persons or entities.

120. (c) *At the EU level*, the UNSCR1267/1989 is implemented through the prohibition to make available funds or economic resources, directly or indirectly, to, or for the benefit of designated persons and entities, to entities owned or controlled directly or indirectly and acting on behalf of

or the direction of those. These requirements are obligatory for the EU nationals and persons and entities within the EU jurisdiction. The prohibition is waived when authorised or notified. This is ensured cumulatively through the provisions of the Council Decision 2016/1693/CFSP (Art.3(2, 5)) and EU Regulation 881/2002 (Art. 2(2-2a), Art.2a and Art.11). The provisions of the UNSCR 1988 are implemented cumulatively through the prohibitions and derogations as set out in the Council Decision 2011/486/CFSP (Art.4(2 and 3) and EC Regulation 753/2011 (Art.3(2) and Art.5). In both instances there is no explicit reference to assets owned jointly.

121. With regard to UNSCR 1373, the prohibitions and derogations are implemented through EU Regulation 2580/2001 (Art. 2(1(b), Art.6 and Art.10). There is no explicit reference to the prohibitions with respect to funds or other assets controlled by, or indirectly, or jointly owned by, or derived from assets owned by, or owned by a person acting on behalf of, or at the direction of a designated person or entity. However, this gap is largely mitigated by the EC's ability to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, Art.2(3) (iii - iv)).

122. While the gap related to the absence of provisions on the assets jointly owned, as identified in all three instances remains, the non-binding EU Best practices for the implementation of restrictive measures (8519/18, para. 34) and EU Council Sanctions Guidelines (para. 55a) clarify this matter.

123. *At the national level*, prohibition is extended to making available financial and economic resources to designated persons, providing a range of defined financial services investment, initiation or continuation of business relationship, and provision of consultancy (ISA, §14(2-8). These prohibitions are therefore limited only to designated persons and to listed activities. Derogations from the prohibitions are regulated pursuant to ISA (§11(2) and §13).

124. (d) *At the EU level*, designations made pursuant to respective EU instruments are published in the Official Journal of the EU. Information on designations is included in the EU Consolidated Financial Sanctions List, which is also available publicly. Once published the measure is enforced, thus immediate communication of EU designations is ensured. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures, which are periodically revised and are made publicly available.

125. *At the national level*, the EFIU shall immediately publish or make available on its website information regarding the imposition or amendments regarding designated persons and entities (ISA, §16(1)). The EFIU (in 2022) and the EFSA (in 2021) have issued respective Guidelines for implementation of financial sanctions. The EFIU Guidelines are addressed to all natural and legal persons in general, and to covered FIs, VASPs and legal service providers only, in particular. The EFSA Guideline is addressed only to its supervised OEs. Hence, those together do not specifically target all FIs and DNFBPs as required by the FATF Standard.

126. (e) *At the EU level,* the reporting obligation is widely covered under the requirement to "provide immediately any information which would facilitate compliance with […] Regulation […]" (EC Regulation 881/2002 (Art. 5(1(a)), EC Regulation 753/2011 (Art.8(1(a)) and EC Regulation 2580/2001, Art.4(1)).

127. *At the national level*, when the persons with special obligations and legal service providers apply financial sanctions, they shall immediately inform about this the EFIU. This includes also intended transactions (ISA, §21(1) and §24(1)). The non-covered FIs, and all other DNFBPs

(including non-covered) are subject to similar requirements within the scope of the provisions addressed to all natural and legal persons (ISA, §19(1)).

128. (f) *At the EU level,* freezing of funds and economic resources or the refusal to make funds or economic resources available, carried out in good faith on the basis that such action is in accordance with the Regulation, shall not give rise to liability of any kind on the part of the natural or legal person, entity or body implementing it, or its directors or employees, unless it is proven that the funds and economic resources were frozen, or not made available, as a result of negligence (EC Regulation 881/2002 (Art. 6), EC Regulation 753/2011 (Art.7(1)). No similar provisions are set in the EC Regulation 2580/2001.

129. *At the national level*, there are no provisions adopted to protect the rights of *bona fide* third parties acting in good faith when implementing the international financial sanctions.

130. ***Criterion 6.6 –*** The procedures for de-listing and unfreezing the funds or assets of persons and entities no longer meeting the designation criteria are implemented in Estonia in a following manner:

131. (a) *At the EU level,* for designations made in line with the UNSCRs 1267/1989 and 1988 mechanisms, there are procedures to consider de-listing requests through EC Regulations (EC Regulation 881/2002, Art. 7c, and EC Regulation 753/2011, Art.11 (3-5)). The process for applying to the EU when listed in on the basis of the UN Sanctions is provided in the EU Sanction Guidelines (5664/18, Annex I, para 18-20) and the EU Best Practices for the effective implementation of restrictive measures (8519/18, para.23-24)).

132. *At the national level*, the MFA is the designated body for submission, of a proposal to the UNSC Committees to remove a natural or legal person, entity or body that does not meet the conditions set out in the resolution (ISA, §8.1(2)).

133. (b) *At the EU level,* for 1373 designations, the EU has de-listing procedures under Regulation 2580/2001 (Art.7). The detailed process for de-listing under the EU autonomous sanctions is provided respectively in the EU Best Practices for the effective implementation of restrictive measures (8519/18, para.18-22)). De-listing is immediately effective and may occur ad hoc or after mandatory 6-monthly review (CP 2001/931/CFSP, Art.1(6) and Regulation 2580/2001, Art.7 and Art.11(2)).

134. *At the national level,* there are various mechanisms for reconsideration of the designations. Under the first mechanism - the sanctions imposed by the Government of Estonia shall be valid until the term designated in a regulation or for an unspecified term. If those are enforced for more that 1 year, they need to be revised regularly. However, the legislator does not specify what is considered as "regularly" for the revision and the process for the revision when initiated (ISA, §29(1-2)). Under the second mechanism - a governmental authority, a state agency administered by a governmental authority, or a court may make a reasoned proposal to the MFA to remove a subject of the sanctions of the Government of the Republic from the list (ISA, §29(4)). While in none of the two instances it is indicated in the ISA who should be the decision-making body with respect to delisting of the designations, authorities suggested that this will be dealt by within the scope of the Administrative Procedure Act (§93(1)). According to the latter, the authority issuing the act within its competences is the one also to repeal it (other than that this can be decided by the Supreme Court).

135. (c) *At the EU level*, a listed individual or entity can write to the EU Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission

Implementing Regulation, or a Council Implementing Regulation in Court, per Treaty on the Functioning of the European Union (TFEU) (Art.263(4)). TFEU (Art.275) also allows legal challenges of a relevant CFSP Decision.

136. *At the national level,* (i) the subject of the sanctions of the Government of Estonia may submit a reasoned application together with evidence to the MFA for removal from the list of subjects of sanction. The MFA shall respond to the inquiry within thirty days (ISA, §28 (2)); and (ii) a person who is the subject of the sanctions of the Government of Estonia may file an appeal regarding the designation of them as the subject of sanction with an Administrative Court pursuant to the procedure provided for by the Code of Administrative Court Procedure (ISA, §28(4)).

137. (d) and (e) *At the EU level*, with regard to designations under 1267/1989 and 1988, designated persons/entities are informed of the listing, its reasons and legal consequences, their rights of due process and the availability of de-listing procedures including the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations). There are procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the EU Council (EC Regulation 881/2002, Art.7a; EC Regulation 753/2011, Art.11).

138. *At the national level,* on the MFA website[247] 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. This webpage also provides information on addressing the UN Office of the Ombudsperson with respect to designations on the Al-Qaida Sanctions Lists.

139. (f) *At the EU level,* upon verification that the person/entity involved is not designated, the funds/assets *must* be unfrozen (EC Regulations 881/2002, 753/2011 and 2580/2001). The EU Best Practices on the implementation of restrictive measures provide guidance on the procedure for cases of mistaken identity (8519/18, para. 8-17).

140. *At the national level,* person with regard to whom TFS has been applied shall have the right to submit an application to the EFIU for verification whether the application of sanctions has been lawful. The EFIU *investigates* and verifies the claims made by the person within 10 working days (or where justified up to 60 days) and immediately informs the person who submitted the application or notice of the results of the inspection (ISA, §17-18). The decision taken by the EFIU can be appealed in court (Code of Administrative Court Procedure, §5(1)).

141. (g) *At the EU level*, legal acts on delisting are published in the EU Official Journal and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission. Once published the measure is enforced, thus immediate communication of EU designations is ensured. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures, which are periodically revised and are made publicly available.

142. *At the national level*, the EFIU shall immediately publish or make available on its website information regarding the imposition or amendments regarding designated persons and entities (ISA, §16(1)). The EFIU (in 2022) and the EFSA (in 2021) have issued respective Guidelines for implementation of financial sanctions extending also to the procedures for un-freezing the funds and other assets. The EFIU Guidelines are addressed to all natural and legal persons in general,

[247] https://vm.ee/en/international-sanctions

and to covered FIs and legal service providers only, in particular. Hence, do not specifically target all FIs and DNFBPs as required by the FATF Standard. The EFSA Guideline is addressed only to its supervised OEs.

143. ***Criterion 6.7 –*** *At the EU level*, there are procedures in place to authorise access to frozen funds or other assets which have been determined to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses (EC Regulation 881/2001, Art.2a; EC Regulation 753/2011, Art.5; and EC Regulation 2580/2001, Art.5-6).

144. *At the national level,* the authorisation is issued by the EFIU on the basis of received application with the approval of the MFA, on the conditions imposed by the UNSCRs (ISA, §9(1), §11(2) and §13(1-2, 4)). The wording of the ISA is broad to cover both types of expenses: basic and extraordinary, as provided by the UNSCR 1452

Weighting and Conclusion

145. Estonia implements the UNSCRs without delay. It has a framework for domestic designations under the UNSCR 1373. The framework for proposing the designations to the UN Committees and to other countries is largely in place. There are moderate shortcomings with respect to requirement for freezing assets, such as limited circumstances in, and assets to which the freezing measures shall be applied. Also, prohibition to make funds available has limitations. The rights of the bona fide third parties are not protected under the domestic legislation. There are minor shortcomings with respect to provision of guidance to OEs and reconsidering the designations. **R.6 is rated PC**

Recommendation 7 – Targeted financial sanctions related to proliferation

146. These requirements were added to the FATF Recommendations in 2012 and were therefore not previously assessed. Estonia implements UNSCRs through the domestic legislation ISA and the EU legislation. UNSCR 1718 concerning the DPRK is transposed into European law by EU Council Decision 2016/84/CFSP, and EC Regulation 2017/1509, and UNSCR 2231 requirements are implemented through EU Council Decision 2010/413/CFSP and EC Regulation 267/2012. The EC Regulations have direct legal effect in Estonia as per general EU law principles. The ISA provisions on implementation of TFS are identical for TF and PF sanction regimes, hence the analysis under R.6 also applies here, where the reference is made.

147. ***Criterion 7.1 –*** *At the EU level,* implementation of TFS, pursuant to UNSCRs 1718 and 2231, does not yet occur "without delay." There is often a delay between the date of the UN designation and its transposition into the EU law. While the sanctions for DPRK are generally not implemented "without delay", the sanctioning system is mitigated by the significant number of other designations by the EU. This does not apply to sanctions for Iran.

148. *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.

149. ***Criterion 7.2*** – In Estonia, the MFA is a coordinating body for implementation of the international sanctions (ISA, §10(1)). The EFIU is a designated authority for implementation and enforcement of the TFS under the Estonian national legislation (ISA, §11(3)3)). The EFSA

exercises supervision over compliance of application of financial sanctions by its supervised OEs (ISA, §30(1.1)). The BA and the MoJ (or when delegated - the CN) carry out supervision of lawyers and notaries (ISA, §30(4),(5)).

150. (a) *At the EU level,* in relation to UNSCRs 1718 and 2231, EU Regulations establish the obligation to freeze all the funds and economic resources belonging to a person or entity designated on the European list (EC Regulation 2017/1509 (Art.1 and 34) and EC Regulation 267/2012 (Art.23, 23a and 49).

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

152. (b) *At the EU level,* the freezing obligation extends to all funds and economic resources belonging to, owned, held or controlled by a designated person or entity (EC Regulation 2017/1509, Art.34; EC Regulation 267/2002, Art.23 and 23a). This includes funds or other assets derived or generated from such funds (EC Regulation 2017/1509, Art. 2(12(d)), EC Regulation 267/2002, Art.1(l(iv))). However, (i) there is no explicit reference to funds or assets owned jointly, but the non-binding EU Best practices for the implementation of restrictive measures (8519/18, para. 34) clarify this matter; (ii) there is no reference to funds or assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities, but (a) these situations are covered by the requirement to freeze funds or assets "controlled by" a designated person or entity and (b) by requiring the designation of any person or entity acting on behalf or at the direction of designated persons or entities (EC Regulation 2017/1509, Art.34(5); EC Regulation 267/2012, Art.23(2(a, c, e)) and 23a (2(c)).

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

154. (c) *At the EU level,* no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of any person or entity designated by EU (EC Regulation 2017/1509, Art.1 and 34(3); EC Regulation 267/2012, Art. 23(3), 23a(3) and 49).

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

156. (d) *At the EU level,* designations made pursuant to respective EU instruments are published in the Official Journal of the EU. Information on designations is included in the EU Consolidated Financial Sanctions List, which is also available publicly. Once published the measure is enforced, thus immediate communication of EU designations is ensured. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures, which are periodically revised and are made publicly available.

157. *At the national level*, the regulatory framework as described under c.6.5(d) apply. The EFIU (in 2022) and the EFSA (in 2021) respective Guidelines for implementation of financial sanctions apply also to PF-related TSF sanction regime and address the same scope of OEs.

158. (e) *At the EU level,* the reporting obligation is widely covered under the requirement to "provide immediately any information which would facilitate compliance with […] Regulation […]" (EC Regulation 2017/1509, Art.50(1(a)); EC Regulation 267/2012, Art.40(1(a)).

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

160. (f) *At the EU level,* the rights of *bona fide* third parties are protected at European level (EC Regulation 2017/1509, Art.54 and EC Regulation 267/2012, Art.42).

161. *At the national level*, there are no provisions adopted to protect the rights of *bona fide* third parties acting in good faith when implementing the international financial sanctions.

162. ***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).

163. *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 BA and the MoJ (or when delegated - the CN) (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).

164. There are various sanctions set forth for the failure to comply with obligations under R.7, but gaps exist.

165. (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 dissuasive and proportionate sanctions set for the non-compliance with the percept set for the covered FIs and other natural and legal persons (thus covering non-covered FIs and all DNFBPs), except for the PSPs, EMIs and credit providers (ISA, §33) (see also c.35.1);

166. (b) Under the misdemeanour proceedings the sanctions set only extend to the violation of a requirement to notify the EFIU of identification of a listed person or entity or submission of false information (ISA, §35). Those cover only persons with special obligations which include only the covered FIs and none of the DNFBPs and do not extent to the violation of an obligation of freeze without delay and without prior notice. Violation of a notification requirement or filing false information is punishable by a fine of up to 300 fine units (EUR 1 200) 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 which affect the effectiveness, proportionality and dissuasiveness of sanction as under c.35.1 apply;

167. (c) Under the disciplinary proceedings the BA and the MoJ and the CN 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 and dissuasive (see also c.35.1);

168. (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 (PC, §93.1). Sanctions are set for both the 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.

169. ***Criterion 7.4*** – (a) *At the EU level*, petitioners of PF TFS can submit de-listing requests either through the UNSCR 1730 Focal Point or through their government (EU Best practices for the implementation of restrictive measures, 8519/18, para. 23).

170. *At the national level,* on the MFA website[248] 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.

171. (b) *At the EU level*, the EU Best Practices on the implementation of restrictive measures provide guidance on the procedure for cases of mistaken identity (8519/18, para. 8-17).

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

173. (c) *At the EU level,* there are procedures for authorising access to funds or other assets if member states' competent authorities have determined that the exemption conditions of UNSCRs 1718 and 2231 are met (EC Regulation 2017/1509, Art.35-36 and EC Regulation 267/2012, Art. 24, 26-28).

174. *At the national level,* the regulatory framework as described under c.6.7 apply.

175. (d) *At the EU level*, legal acts on delisting are published in the EU Official Journal and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission. Once published the measure is enforced, thus immediate communication of EU designations is ensured. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures, which are periodically revised and are made publicly available.

176. *At the national level,* the EFIU shall immediately publish or make available on its website information regarding the imposition or amendments regarding designated persons and entities (ISA, §16(1)). The EFIU (in 2022) and the EFSA (in 2021) respective Guidelines for implementation of financial sanctions apply also to PF-related TSF sanction regime and address the same scope of OEs.

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

178. (a) *At the EU level,* the addition of interests or other earnings to frozen accounts is permitted pursuant to EC Regulation 2017/1509, Art.34(9) and EC Regulation 267/2012, Art.29).

179. *At the national level*, there is no provision 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.

180. (b) *At the EU level,* with regard to freezing measures adopted on the basis of Resolutions 1737 and 2231, specific provisions allow for the payment of sums due by virtue of contracts concluded prior to listing, provided that the payment is not related to an activity prohibited by the resolutions, and that the UN Sanctions Committee is notified in advance (EC Regulation 267/2012, Art. 25).

181. *At the national level,* the authorisation is issued by the EFIU on the basis of received application with the approval of the MFA, on the conditions imposed by the UNSCRs (ISA, §9(1), §11(2) and §13(1-2, 4)). The wording of the ISA is broad to cover authorisation for making payments under the contracts arisen prior to the listing of person or entity pursuant to UNSCR 1737 and 2231

[248] https://vm.ee/en/international-sanctions

Weighting and Conclusion

182. Estonia implements the UNSCRs on PF in a timely manner. There are moderate shortcomings with respect to requirement for freezing assets, such as limited circumstances in, and assets to which the freezing measures shall be applied also, prohibition to make funds available has limitations. There are various sanctions set forth for the failure to comply with obligations under R.7, but moderate limitations exist. The rights of the *bona fide* third parties are not protected under the domestic legislation. There are minor shortcomings with respect to provision of guidance to OEs and reconsidering the designations. **R.7 is rated PC.**

Recommendation 8 – Non-profit organisations

183. In the 4th round MER of 2014, Estonia was rated LC on former SRVIII due to the absence of effective supervision of the NPO sector and limited outreach to the NPO sector. As the requirements in R.8 have changed significantly since then, the previous analysis is no longer relevant.

184. ***Criterion 8.1*** – a) The NPO sector was considered within the scope of the NRA conducted in 2020. According to the findings of the NPO risk assessment it is stated that the majority of NPOs are considered low risk due to the types of activities conducted. While the NRA reflects in general on the overall risk state in the NPO sector, authorities suggested that the subset of the NPOs that would fall within the scope of higher risk entities would be the ones caring out religious and charity activities, especially where raising funds. Within the scope of the NPO risk assessment relevant vulnerabilities were assumed (raising funds in cash and VAs). Further to the NRA 2021, the ISS determined that 56 NPOs (3 foundations and 53 non-profit associations) are at a higher risk of TF. This understanding was explained in the "Overview of the Non-Profit Sector at a Higher Risk of Terrorist Financing" published in April 2022. These findings while commendable, have important gaps and do not clarify the reached conclusions. (see IO.10).

185. (b) Estonia did not identify the nature of the threats posed by terrorist entities to the NPOs which are at risk, as well as how these can be abused. The only Estonia specific and concrete example was made with respect to work migrants employed by their compatriots.

186. (c) Estonia has not reviewed the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for TF support. Estonia amended recently the MLTFPA: the threshold of cash transactions for which the NPOs shall file a transaction report to EFIU was lowered and a requirement to do so also when higher ML/TF risk factors are observed added, i.e., treating the NPOs as the OEs with limited obligations. This is a positive step towards improving the monitoring and detection of higher-risk transactions, and potentially improving the NPOs awareness and capacities to identify potential TF. Nevertheless, this measure does not suggest amounting to targeted approach towards 56 higher risk NPOs.

187. (d) The assessment of the NPO sector is conducted within the scope of the NRA in 2021, for the years 2017-2019. This was followed by the ISS analysis of the NPO sector and publication of a document - "Overview of the Non-Profit Sector at a Higher Risk of Terrorist Financing" published in April 2022. The regularity of reassessment of risks is decided by the authorities, and expected to be conducted upon necessity.

188. ***Criterion 8.2*** – (a) According to the Statutes of the Ministry of the Interior (§20), is organising matters related to religious associations, the Ministry contributes to the development of relations between the state and local governments and religious associations and their

structural units and to solving economic, social, educational and cultural problems, participates in developing strategies necessary to achieve common interests religious associations. The Ministry of the Interior selected four strategic partners through a public competition to help implement the program "Community Estonia" in 2021-2024. There were several NPOs identified to implement the program as strategic partners of the Ministry of the Interior for the next four years.

189. (b) The MoI conducted a Risk mitigation seminar to religious associations (in 2021). ISS also conducted a CFT training with churches and religious congregations (in 2021). These trainings, nevertheless, yet covered the small fraction of entities. The EFIU published its NPO study in 2022 and sent it also to LEAs, supervisory authorities, ministries, larger NPOs, umbrella organisation of the NPO, as well as published on the EFIU's webpage. The NPOs were not aware of the NRA results and the EFIU study.

190. (c) Based on the findings of the NRA 2020 that were established, *inter alia*, based on the responses of the NPO sector and thus based on the vulnerability of the sector, the EFIU changed its guidance on TF reporting and provided specific indicators to the NPO sector, the EFIU also provided a trends and typologies section in its NPO analysis from 2022.

191. (d) Estonia did not yet implement measures for encouraging the NPOs to conduct their transactions through formal financial channels.

192. ***Criterion 8.3*** – There are two mechanisms set in the country for supervision and monitoring of the NPOs. The ETCB conducts the monitoring of NPOs from the tax revenue perspective. This monitoring does not set risk-based approach aimed at tackling higher vulnerability NPOs, but has a specific, tax-compliance monitoring perspective. The second supervisory authority is the EFIU. This comes into the play when the NPO conducts transactions which bring them under the scope of the MLTFPA. Under these conditions, the regulatory framework requires that the EFIU conducts risk-based supervision of implementation of preventive measures in the capacity of the OE. So far, the NPOs did not fall under the competence of the EFIU since they did not report to conduct cash transactions of a reportable threshold. While the mechanisms in place can contribute to monitoring and supervision of the NPOs in general, these are not mechanisms that would ensure that Estonia adequately meets the requirements under the criterion, since those do not amount to risk-based measures applied to NPOs at risk of terrorism financing abuse.

193. ***Criterion 8.4*** – The EFIU is the competent authority to conduct supervision over the NPOs for implementation of the MLTFPA, in the circumstances described in c.8.2(d), according to the provisions of the MLTFPA (§54(4)). As also described above, the ETCB conducts the monitoring of NPOs from the tax revenue perspective, applying the risk-based metrics which are not relevant to the subject matter of R.8.

194. (b) EFIU as a supervisory authority has the power to apply sanctions and issue administrative or misdemeanour proceedings against NPOs, except for delicencing and de-registration (see also R.35). These sanctions, while relevant for the obligations set for NPOs under the MLTFPA, nevertheless are not entirely relevant for non-compliance with implementation of requirements under R.8. No information was provided with respect to sanctions applied by the ETCB for non-compliance with implementation of requirements under R.8.

195. ***Criterion 8.5*** – (a) Cooperation, coordination and information sharing among the competent authorities, namely ISS and FIU is carried out on the basis of MLTFPA (§62). The EFIU is responsible for coordinating international and domestic cooperation regarding the countering

of TF. The EFIU has access to all relevant databases, the right to obtain information from all stakeholders and from the ISS (SAA, §31, §31.1 and §32).

196. (b) So far, no links of NPOs to terrorist groups or organisations, terrorism-related individual, or terrorism financing by exploiting or abusing their capabilities have been detected. ISS according to SAA (§6(2.1)) of the is capable to investigate TF offences using range of investigative techniques.

197. (c) According to the provisions of the CCP (§86, §91, and §215) ISS have powers to have access to financial, administration and management data of NPOs. The information contained in the BO register is accessible by the ISS (SAA, §31-1).

198. (d) EFIU carries out activity, including the supervision of the NPO sector in certain circumstances. If suspicions arises that an NPO is involved in TF activities or its being misused for TF purposes, this information referred to LEAs for investigation.

199. ***Criterion 8.6*** – Estonia indicates that country had identified specific points of contact and procedures to respond to international requests for information regarding particular NPOs falling under the FATF definition suspected of terrorist financing or involvement in other forms of terrorist support. Estonia appointed ISS as a contact authority to develop cooperation with foreign police and security services (Statute of the ISS, Art.8). Estonia also relies upon existing mechanisms for international cooperation (via FIU-to-FIU and other means for communication)

Weighting and Conclusion

200. It is acknowledged that Estonia made efforts to identify the subset of NPOs vulnerable for TF abuse. These efforts of authorities are commendable, but major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including identification of the specific subset of the NPOs. Gaps remain with the review of adequacy if measures to address the vulnerable subset of NPOs. Improvements are required with respect to the supervisory and monitoring framework to ensure those are risk-based and addressing the target group. This affects respectively the sanctioning requirements.**R.8 is rated PC**.

Recommendation 9 – Financial institution secrecy laws

201. In the 4th round MER of 2014, Estonia was rated LC on former R.4. The technical issues identified were with regard to uncertainty in interpretation of the provisions relating to sharing of information between financial institutions

202. *(a) Access to information by competent authorities*:

203. The EFIU and the ISS have the right to obtain secret information in the cases and to the extent prescribed in the MLTFPA and the International Sanctions Act (ISA) (Credit Institutions Act (CIA), §88(4^2(1)).

204. LEAs and the PO has the right to obtain secret information based on the request, once criminal investigation is initiated (CIA, §88(5(2))), as well as based on a request for MLA received from a foreign state.

205. Supervisors (the EFSA and the EFIU) obtain data without limitations (regardless of if they carry out onsite inspection or not) (MLTFPA, §66 and CIA, §88(4^1)).

206. *(b) Sharing of information between competent authorities domestically*

207. To prevent or identify ML/TF or related predicate offence and to facilitate investigation, the EFIU is obliged to disseminate information, including information subject to tax and banking secrecy to the PO, LEAs, and the court (MLTFPA, §60).

208. In addition, for credit institutions, it is provided that banking secrecy will not be ground for refusal to disclose information to the BoE (CIA, § 88), the EFSA and to the financial supervision authority of a foreign state through the EFSA, the European Central Bank, the EFIU and the ISS (based on the MLTFPA and ISA), as well as to the ETCB and to the PBGB (based on the Identity Documents Act, §88(51)).

209. *(c) Sharing of information between competent authorities internationally.*

210. The EFSA can share secret information with foreign counterparts (Financial Supervision Authority Act, §47(2)). Also, there are legal provisions enabling the EFIU to cooperate internationally including when exchanging secret information (MLFTPA, §63(2)). Concerning the LEAs and PO, exchange of secret information is regulated by CIA (§ 88).

211. *(d) Sharing of information between financial institutions*

212. The prohibition of exchange of confidential information does not apply if such information has been exchanged between credit institutions and FIs in between themselves whereas they are part of the same group (MLTFPA, §51).

Weighting and Conclusion

213. **R. 9 is rated C.**

Recommendation 10 – Customer due diligence

214. In the 4th round MER of 2014, Estonia was rated LC on former R.5. The identified technical deficiencies related to: (i) the absence of a clear requirement to determine whether the customer is acting on behalf of another person and of the obligation to apply CDD requirements to existing customers on the basis of materiality and risk and (ii) the need to clarify in the law the requirements to verify the identity of the beneficial owner, to identify and verify the identity of the beneficiary under the policy and to ensure that transactions undertaken throughout the business relationship are consistent with the institution's knowledge of the customer and their business and risk profile.

215. Since then, a new law was adopted on 26 October 2017 (the MLTFPA), which has undergone a number of changes, including most recently on March 2022. In 2018, based on § 57(1) of the MLTFPA, the EFSA issued AML/CFT Advisory Guidelines which explain the content of and compliance with the requirements provided for in the MLTFPA (and other related legislative acts, including those adopted at the EU level) and provide guidance to the FIs under its supervision (EFSA AML/CFT Guidelines, §2.1.2.). The application of the rules prescribed by the Guidelines are subject to the "comply or explain" principle, pursuant to which the FIs may not implement fully or partially some points of the Guidelines but must be able to justify the decision (EFSA AML/CFT Guidelines, §2.1.2.). If the provisions of the Guidelines are in conflict with the imperative legislation, the requirements arising from the legislation will prevail. In May 2022 the EFIU also issued similar AML/CFT Guidelines, pursuant to §56(1) of the MLTFPA. The Guidelines do not contain a legal basis for enacting their provisions and, therefore, they do not qualify as an *enforceable means*. The references to the EFSA and EFIU AML/CFT Guidelines in relation to R.10 is made with the purpose to highlight the clarifications brought out by the Guidelines.

216. The following activities which are covered by the FATF definition of FIs are not subject to the MLTFPA obligations: companies managing a mandatory pension fund and life insurance companies providing services related to mandatory funded pension insurance contracts within the meaning of Funded Pensions Act.

217. ***Criterion 10.1*** – FIs are prohibited from opening or maintaining anonymous accounts (including saving books or safe-deposits) or accounts (including saving books or safe-deposits) in fictitious names. A transaction violating this prohibition is void (MLTFPA, §25(1), (2)).

218. ***Criterion 10.2*** – (a) FIs are required to undertake CDD measures when establishing business relationship (MLTFPA, §19(1)1)).

219. (b) FIs are required to undertake CDD measures when carrying out an occasional transaction above EUR 15 000 or an equivalent sum in another currency whether carried out in a single transaction or several related payments over a period of up to one year (MLTFPA, §19(1)2)). Additionally, FIs are also required to apply CDD measures when carrying out occasional transactions over EUR 1000 or an equivalent value in another currency whether it is performed in a single transaction or several linked payments (MLTFPA, §25(1^1)). It remains unclear which of the two requirements would prevail.

220. (c) FIs are required to undertake CDD measures when carrying out an occasional wire transfer exceeding EUR 1 000 whether carried out in a single transaction or several linked payments over a period of up to one month (MLTFPA, §19(4)). As described under R.16 c.1, the Regulation (EU) 2015/847 and the MLTFPA do not cover the transfers equivalent to EUR 1000.

221. (d) FIs are required to undertake CDD measures upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits available (MLTFPA, §19(1)4).

222. (e) FIs are required to undertake CDD measures when there are doubts as to the "sufficiency or truthfulness" of the documents or data previously obtained (MLTFPA, §19(1)3)).

223. ***Criterion 10.3*** – FIs are required to identify the customer and verify customer's identity based on information obtained from a "reliable and independent source", including using means of electronic identification and of trust services for electronic transactions. The requirement applies to permanent or occasional customers (MLTFPA, §20(1)1)).

224. ***Criterion 10.4*** – FIs are required to identify and verify the identity of the representative of a customer or person participating in an occasional transaction and to confirm their right of representation (MLTFPA, §20(1)2)).

225. ***Criterion 10.5*** – FIs are required to identify the BO and to take measures for the verification of their identity to the extent that allows them to make certain that they know who the beneficial owner is, and they understand the ownership and control structure of the customer (permanent or occasional) (MLTFPA, §20(1)3)). The MLTFPA does not provide for the obligation to verify the BO's identity based on information and data obtained from a *reliable source*. For legal entities customers, the EFSA and the FIU AML/CFT advisory Guidelines detail the reliable sources for the verification of the BO information, which include the original of the registration documents, certified copies, data obtained from registers (CR, register of NPO or other relevant registers of foreign countries), as well as other publicly accessible and/ or reliable sources that are sufficient to make it possible to conclude who the beneficial owner is (EFSA AML/CFT Guidelines, §4.3.3.11; EFIU AML/CFT Guidelines, §4.3.3.11 and 4.3.1.17). As explained in the introduction to this recommendation, these Guidelines are not considered enforceable means.

226. "Beneficial owner" means a natural person who, via ownership or other type of control, has the 'final dominant influence' over a natural or legal person, or in whose interests, for the benefit of whom or in whose name a transaction or operation is made (MLTFPA, §9(1)).

227. ***Criterion 10.6*** – Covered FIs are required to understand and, where relevant, obtain information on the business relationship, and occasional transaction or operation (MLTFPA, §20(1)4)). This shall include understanding of the purpose of the business relationship or of the occasional transaction, identifying, inter alia, the permanent seat, place of business or place of residence, profession or field of activity, main contracting partners, payment habits, whether they act for or on behalf of another and, in the case of a legal person, also the experience of the customer or person participating in the occasional transaction (MLTFPA, §20(2)). The obligation to ascertain the purpose and nature of the business relationship is confirmed by the EFSA AML/CFT Guidelines, being described as a "significant" part of the implementation of the KYC principles (§4.3.6.1.).

228. ***Criterion 10.7*** – (a) Covered FIs are required to conduct ongoing monitoring of a business relationship (MLTFPA, §20(1)6)). This shall include checking transactions made during a business relationship in order ensure that they are in concert with the knowledge of the customer, its activities and risk profile, as well as identifying the source and origin of funds used in a transaction (MLTFPA, §23(2)).

229. (b) Covered FIs are required to ensure that the relevant documents, data or information obtained under the CDD process is regularly updated (MLTFPA, §23(2)2)). The FIs are required to establish the principles for monitoring a business relationship when implementing the obligations linked to the rules of procedure and internal control that allow for effective mitigation and management of ML/TF risks (MLTFPA, §23(1), §14(1)). For the FIs supervised by the EFSA, there is an explicit obligation to verify more frequently, at least once a year, the customers and business relationships whose risk is higher than usual (EFSA AML/CFT Guidelines, §4.4.1.2.).

230. ***Criterion 10.8*** – Covered FIs must understand the ownership and control structure of the customer (permanent or occasional) (MLTFPA, §20(1)3)). This applies to all customers whether they are legal or natural persons. For customers that are legal persons and legal arrangements, in order to understand the ownership and control structure, the FIs may rely on the statements or written explanations of the representatives of the legal entity or trust, civil law partnership, community or other similar legal entity, excepting the situations when there are doubts as to the accuracy of the information (e.g., contradicting the BO information) (EFSA AML/CFT Guidelines, §4.3.3.14.). The covered FIs are required to understand the customer's purpose and intended nature of the business relationship, including the permanent seat, place of business or place of residence, field of activity, main contracting partners, payment habits, the experience of the customer or person participating in the occasional transaction (MLTFPA, §20(1)4), (2)).

231. ***Criterion 10.9*** – The following information must be obtained by the FIs for customers that are legal persons: (a) name or business name, the registry code or registration number and the date of registration (MLTFPA, §22(1)1) and 2)). There is no express obligation to obtain information on the legal form of the legal person. The EFSA and EFIU AML/CFT advisory Guidelines specify that the information on the legal form would be obtained in relation to the name/ business name of the legal entity – "business name or name (with the legal form)" (EFSA AML/CFT Guidelines, §4.3.2.6; EFIU AML/CFT Guidelines, §4.3.2.6); (b) the names of the director, members of the management board or other body replacing the management board. There is no requirement to obtain the governing instrument (such as the memorandum or articles of

association) of a customer who is a legal person, but §20(1)3) demands the obliged entity to make certain that it understands the ownership and control structure of the customer and §22(1)3) requires that the managements authorisation in representing the legal person must be collected; c) there is no obligation to obtain the information on the registered office/ place of business during the identification process of a legal entity described under §22 of the MLTFPA. However, this data must be obtained by the FIs in the context of understanding the business relationship or the occasional transaction by "identifying, *inter alia,* the permanent seat, place of business or place of residence…" (MLTFPA, §20(2)4)).

232. For customers that are legal arrangements, the applicable CDD measures are those required for natural persons (name, personal identification code or, where none, the date of birth and the place of residence), described under §21(1) of the MLTFPA, supplemented by the obligation to gather enough information on the beneficiaries of a trust or legal arrangement (MLTFPA, §28). None of the CDD measures under the law requires the FIs to obtain information such as proof of existence or the powers that regulate and bind the legal arrangement. However, under the record keeping obligation, the FIs have to obtain and keep an extract of the registry card or a certificate of the registrar of the register where the legal arrangement has been registered (MLTFPA, §46(6)). The EFSA and EFIU AML/CFT Guidelines, provide that, when verifying the identity of the BO of a trust or other legal arrangement, the FIs have to obtain *inter alia* the trust deed and letter of wishes (EFSA AML/CFT Guidelines, §4.3.3.13; EFIU AML/CFT Guidelines §4.3.3.13). This is not sufficient to comply with the requirement under c.10.9.

233. ***Criterion 10.10*** – The requirement to identify and verify the BO information is described under c.10.5. In the case of legal persons, this shall be done through the following information:

234. (a)-(b) the identity of the natural person who has the "final dominant" influence over the legal person via *ownership* or *other type of control,* irrespective of the size of share, voting or ownership rights or direct or indirect nature (MLTFPA, §9(1)1)). Unlike the standard, which requires that the measures for identifying the ultimate controlling interest, via ownership and other type of control, have a "cascading" nature[249], the obligation under §9(1)1)) appears to offer two alternative options. When the BO of a company is a trustee, all persons specified under c.10.11 are considered to be BOs and must be identified and verified (MLTFPA, §9(4^2)).

235. (c) Where a natural person cannot be identified after all possible means of identification have been exhausted or where there are doubts as to whether the identified person is the BO, the FIs will identify the natural person who holds the position of a senior managing official. Where several persons meet this term, the BO will be considered the (i) person(s) who exercise(s) actual control over the company and make(s) strategic decisions or, in absence of such persons, (ii) person(s) who perform(s) day-to-day and regular management of the company (MLTFPA, §9(4), (4^1)).

236. ***Criterion 10.11*** – (a) and (b) The obligation to identify and verify the BO is described under c.10.5. In the case of trusts and other legal arrangements, the following persons who are considered the BO of a trust or other types of legal arrangement shall be identified and verified: (i) the settlor of the trust or the establisher of the arrangement; (ii) the trustee; (iii) the person ensuring and controlling the preservation of property, where such person has been appointed; (iv) the beneficiary, or where the beneficiary or beneficiaries are yet to be determined, the class of persons in whose main interest such trust or arrangement has been set up or operates; (v) any

[249] Each to be used where the previous measure has been applied and has not identified a BO, IN to R.10, footnote 65.

other person who in any way exercises ultimate control over the property of the trust or arrangement (MLTFPA, §9(6)). In the case of the beneficiary of a trust or legal arrangement (iv), the FIs shall gather "enough information" in order to be certain that they are able to definitely identify the beneficiary at the time of making a payment or once the beneficiary exercises their rights.

237. ***Criterion 10.12*** – For life insurance policies, FIs are required to undertake the following measures: (a) for beneficiaries who are identified as specifically named natural persons or legal entities, they must retain the name of the beneficiary, which is identified without delay after the determination of the determination or learning of the person; (b) for beneficiaries whose identity is established based on certain characteristics or in any other manner, sufficient data must be gathered on the circle of persons in such a manner so that it is proven that the identity of the beneficiary can be established at the time of making a payment; (c) in both cases the identity of the beneficiary is verified at the time of making the payment (MLTFPA, §26).

238. ***Criterion 10.13*** – There is a general obligation for the FIs to determine the scope and the exact manner of application of the CDD measures, including the enhanced CDD, based on the previously assessed risk of ML/TF or those relating to a specific business relationship or occasional transaction, operation or person (MLTFPA, §20(6), §36(3)). The MLTFPA does not include the beneficiary of the life insurance policy among the factors characterising a higher risk (described under §36(2), §37), except for the cases when the beneficiary of the life insurance policy or the BO of the beneficiary is a PEP. In this case, additional enhanced measures would be required which include informing the senior management before making the payment and checking the entire business relationship in detail (MLTFPA, §41 (2)). The law also defines the lower risk factors in relation life insurance policy where the simplified CDD measures may be applied – a life insurance contract with a small insurance premium (MLTFPA, §35(2)1)). The EFSA AML/CFT advisory Guidelines prescribes for the covered FIs supervised by EFSA more detailed recommendations in relation to life insurance products. Considering the customer's risk profile and associated risks, as well as the risk assessment of the obliged entity, the FIs shall undertake a series of measures in order to identify complicated, high-value and unusual transactions which would require enhanced CDD. This includes the identification of the connection between: (i) the policyholder and the insured person (ii) the policyholder and the beneficiary, (iii) insured person and the beneficiary, as well as the justification and the understandability of such connections (§ 4.7.1.7.).

239. ***Criterion 10.14*** – Covered FIs are required to verify the identity of the customer and BO before the establishment of a business relationship or the making of a transaction outside a business relationship (MLTFPA, §19(5)). As an exception, they are permitted to complete the verification of the identity of the customer or BO after the establishment of a business relationship when there is a lower ML/TF risk, namely in the case of: (i) limited-use accounts and (ii) circumstances justifying the application of simplified due diligence measures. The limited-use accounts refer to opened accounts before the application of the verification measures where transactions cannot be made until the full application of CDD, as well as to accounts opened for a company during the process of its incorporation provided that the account is credited via an account opened in a credit institution/ foreign branch operating in a EEA state and that it is not debited before the completion of the registration procedure. In both cases, verification must be completed as soon as reasonably possible, and not later than within six months in the second situation (MLTFPA, §27). When applying the simplified CDD, the FIs may verify the identity of the customer at the time of establishment of the business relationship, provided that: (i) it is

necessary for not disturbing the ordinary course of business and (ii) the verification is carried out as quickly as possible and before the taking of binding measures (MLTFPA, §33(1)).

240. ***Criterion 10.15*** – There is no explicit requirement that FIs should adopt risk management procedures concerning the exceptions described under c.10.14. This would be covered by the general requirement to establish procedures for the application of CDD measures (SDD and EDD) and by the obligation to ensure that the CDD measures specified by the internal rules of procedure comply with the risk assessment of the entity and that the FI is prepared to explain them to the supervisory authority (MLTFPA, §14(1)1), §20(8)). The conditions under which a customer may establish a business relationship are described under c.10.14.

241. ***Criterion 10.16*** – The MLTFPA of 2017 specifically established the obligation for the obliged entities to re-apply the new CDD requirements to the existing customers over a period of one year from the entry into force. The FIs had to take into account the importance of the customer the risk profile, as well as the time that has passed from the previous application of the CDD measures or the scope of their application (MLTFPA, §100). A similar obligation was prescribed by the subsequent amending act of the MLTFPA of 2020 in relation to verification of details of beneficial owner (MLTFPA, §100[1]). Other amendments of the MLTFPA (about nine during the period of 2018-2021) appear not to impose such obligations.

242. There is also a general requirement for the covered FIs to update regularly the relevant documents, data or information gathered in the course of application of due diligence measures, based on its risk assessment (MLTFPA, §23(2)2)). The EFSA and the EFIU AML/CFT Advisory Guidelines provide that the updating process must be carried out more frequently for the customers who pose a higher risk, at least once a year. However, this timeframe does not take into account the date that the new national requirements are brought into force. The manner in which the data are updated is to be decided by the FI, based on the risk of the customer and of the business relationship (EFSA AML/CFT Guidelines, §4.4.1.1. – 4.4.1.3; EFIU AML/CFT Guidelines, §4.4.1.2).

243. ***Criterion 10.17*** – Covered FIs are required to perform EDD in order to adequately manage and mitigate "higher-than-usual" ML/TF risks (MLTFPA, §36(1)). A non-exhaustive list of circumstances and factors characterising a higher risk is described under §36(2) and §37(2)-(4) of the MLTFPA.

244. ***Criterion 10.18*** – Covered FIs are permitted to apply simplified CDD measures where a "lower than usual" risk has been identified, based on the national and FI's risk assessments. The lower risk of a transaction/operation or customer has to be established by the FIs before the application of the SDD measures. The FIs must ensure sufficient monitoring of transactions, operations and business relationship so that it would be possible to identify unusual transactions and submit STRs (MLTFPA, §32). A non-exhaustive list of circumstances and factors characterising a lower risk is described under §34(2)(3) and §35(2) of the MLTFPA.

245. ***Criterion 10.19*** – (a) Covered FIs are prohibited from establishing or continuing a business relationship or carrying out an occasional transaction if they are unable to apply the required CDD measures. An agreement established contrary to this prohibition is considered void (MLTFPA, §42(1)(4)(5)).

246. (b) The covered FIs are required to consider submitting a STR when they are unable to comply with the required CDD (MLTFPA, §49(2)).

247. ***Criterion 10.20*** – There is no express legal provision to permit the FIs not to complete CDD in cases where there is a ML/TF suspicion and reasonable belief that performing the CDD process would tip-off the customer. Although not provided in relation to the risk of tipping-off the customer, the covered FIs are permitted not to complete the CDD in the following cases: (i) *concerning the customer relationship* - in case when they receive from the EFIU a specific instruction to continue the business relationship or the establishment of the business relationship, which can potentially also cover situations involving the risk of tipping-off. However, this is limited by the condition of a prior filed STR (MLTFPA, §42(6)); and (ii) *concerning customer transactions* – when the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction, or it may impede catching the suspect. The requirement to submit an STR thereafter remains (MLTFPA, §49(6)).

Weighting and Conclusion

248. Most of the essential criteria are either met or mostly met (13 M and 3 MM). The identified moderate shortcomings refer to the: insufficiency of the information that is required to be obtained in order to identify and verify the identity of customer legal person and legal arrangement (c.10.9); no explicit requirement to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable for reasons other than being identified as a PEP (c.10.13); the obligation to apply the new CDD measures to existing customers is not prescribed in all cases (c.10.16); the permission not to pursue the CDD process when there is a reasonable belief that there is a risk of tipping-off the customer is not established expressly by law and the possibility not to complete the CDD process in relation to customer relationship is limited by the condition of a prior filed STR (c.10.20). The exemptions from the scope of application of the MLTFPA are considered minor due to the low ML/TF risk and the materiality of the sector (see also 26.1). **R. 10 is rated LC.**

Recommendation 11 – Record-keeping

249. In the 4th round MER of 2014, Estonia was rated LC on former R.10. The deficiency was that no provision in the laws or regulations ensure that the mandatory record-keeping period may be extended in specific cases upon request of competent authorities (as preventive measures). Since the last MER, Estonia adopted a new MLTFPA in 2017 with subsequent amendments.

250. ***Criterion 11.1*** – FIs should retain documents on transactions for at least 5 years following the completion of a transaction (MLTFPA, §47(1)(3)).

251. ***Criterion 11.2*** – FIs shall retain all information obtained through the CDD measures, including customer identifications, business correspondence, monitoring of business relationship and internal documents concerning any decisions taken within a FI for at least 5 years following the end of a business relationship or the execution of occasional transaction. The supervisory authorities can request retention of these documents for a longer period, but not more than for another 5 years after the expiry of the first term (MLTFPA, §47(1)(2)(7)).

252. ***Criterion 11.3*** – FIs shall retain all documents as required per c.11.1 and 11.2 (MLTFPA, §46(3)) sufficient to permit reconstruction of individual transactions. In addition, information should be kept in a manner that allows for exhaustively and without delay respond to the requests of EFIU, EFSA, LEAs and PO or courts (MLTFPA, §47(4)).

253. ***Criterion 11.4 –*** FIs shall retain the documents and data in a manner that allows to swiftly make that information available to competent authorities (MLTFPA, §47(4)).

Weighting and Conclusion

254. **R.11 is rated C.**

Recommendation 12 – Politically exposed persons

255. In the 3rd round MER, Estonia was rated LC on former R.6. The 4th round MER of 2014 did not reassess Estonia's compliance with former R.6.

256. The introduction to R.10 lists the activities to which the MLTFPA does not apply.

257. ***Criterion 12.1*** – Both foreign and domestic PEPs seem to be covered by the definition of PEP, as MLTFPA, §9[1] does not distinguish between foreign or domestic PEPs. The definition also includes the persons who have performed prominent public functions and with regard to whom related risk remain. Where a PEP no longer performs important public functions placed upon them, the obliged entity must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk-based measures as long as it is certain that the risks characteristic of PEPs no longer exist in the case of the person (MLTFPA, §41(3)). Thus, the following obligations are mandatory for at least one year after the person is no longer entrusted with prominent public functions. After this period, the obliged entity is required to apply the measures on risk basis.

258. (a) FIs are required to establish rules of procedures for mitigating the ML/TF risk, including instructions for effectively identifying whether a person is a PEP, including a foreign PEP (MLTFPA, §14(5)). FIs are required to gather information on whether a person is a PEP, their family member or a close associate, without a specification with method(s) shall be use for determining whether a person is a PEP (MLTFPA, §20(5)). For the FIs supervised by the EFSA, the EFSA AML/CFT Guidelines clarify that a higher risk level must always be determined and enhanced, and other relevant due diligence measures must be applied if the customer or the BO is a PEP and describes the risk management system to identify a high-risk PEP (§§4.2.6, 4.3.14-4.3.4.17).

259. (b) FIs are required to obtain senior management approval for establishing or continuing a business relationship where the customer or the BO is a foreign PEP (MLTFPA, §41(1)1)).

260. (c) FIs are required to obtain measures to establish the origin of the wealth and the sources of the funds that are used in the business relationship or upon making occasional transactions, when the customer or the BO is a foreign PEP (MLTFPA, §41(1)2)).

261. (d) FIs are required to conduct enhanced ongoing monitoring of the business relationship in relation with foreign PEPs (MLTFPA, §41(1)3)).

262. ***Criterion 12.2*** – (a) The definition of PEP does not distinguish between domestic and foreign PEPs. FIs are required to have procedures for effectively identifying whether a person (the customer or BO) is a PEP (MLTFPA, §14(5), §20(5)). The director, deputy director and a member of a management body of an international organisation are deemed to perform prominent public functions and considered as a PEP. (MLTFPA, §9(2)10)).

263. (b) The measures described under c. 12.1 (b – d) are applicable.

264. ***Criterion 12.3*** – FIs are required to apply the measures under c. 12.1 and 12.2 in relation to family members and close associates of PEPs (MLTFPA, §41(1)). MLTFPA defines the categories of persons that are considered family members of a PEP and close associates (MLTFPA, §9[1] (8)(9)). However, siblings are not covered as family members of a PEP.

265. ***Criterion 12.4*** – In relation to life insurance policies, FIs are required to take measures in order to establish not later than upon making a payment whether the beneficiary of the life insurance policy or the BO of the beneficiary is a PEP, a family member or a close associate. The FIs are also required, in addition to the CDD measures, to apply enhanced measures by: (i) informing the senior management before making the payment and (ii) checking the entire business relationship in detail (MLTFPA, §41(2)). The indicators for suspicions do not include life insurance policies that have been identified as linked to PEPs.

Weighting and Conclusion

266. Only minor shortcomings have been identified. Siblings are not covered as family members of a PEP. The indicators for suspicions do not include life insurance policies that have been identified as PEPs. The underlined shortcomings described under the conclusion to R.10 with regard to the scope of application of the MLTFPA are relevant here. **R. 12 is rated LC**.

Recommendation 13 – Correspondent banking

267. In the 3rd round MER, Estonia was rated LC on former R.7. The evaluation team noted that there were no specific provisions which clearly required understanding respondent bank's business, no clear requirements to obtain approval from senior management before establishing new correspondent relationship, the MLTFPA allowed for simplified measures for correspondent banking relationships with FIs of EU member countries and the FIs were not required to detail the banks' obligation regarding all the AML/CFT responsibilities of each institution. The 4th round MER of 2014 did not reassess Estonia's compliance with former R.7.

268. ***Criterion 13.1*** – Correspondent relationship is defined as the "consistent and long-term" provision of banking services by a bank (correspondent institution) to another bank (respondent institution), including providing a current account, liability account or other account service or other related services such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange service, and a similar business relationship between and among FIs including relationships established for securities transactions or funds transfers (MLTFPA, §7). In cross-border correspondent relationship with a respondent institution of a third country, i.e., outside the EEA, in addition to the CDD measures, FIs are required to:

269. (a) gather sufficient information on the respondent institution in order to fully understand the nature of their activities and, based on publicly available information, make a decision on the reputation and quality of supervision, including researching whether any proceedings have been initiated against the institution in connection with breaching the AML/CFT legislation (MLTFPA, §40(1)1));

270. (b) assess AML/CFT control systems implemented by the respondent institution (MLTFPA, §40(1)2));

271. (c) receive prior approval from the senior management to establish new correspondent relationship (MLTFPA, §40(1)3));

272. (d) document the relevant duties and obligations of both institutions (MLTFPA, §40(1)4)).

273. For correspondent relationships within the EEA, a risk-based approach is taken (MLTFPA, §40(1)), which is not in line with R.13, which requires that the application of the measures established under 13.1 (a)-(d) to all cross-border correspondent banking relationships.

274. ***Criterion 13.2*** – With respect to "payable-through accounts", FIs are required to make certain that that the respondent institution: (a) has verified the identity of the customers and applies CDD measures to them at all times; (b) upon request, is able to present the relevant CDD information (MLTFPA, §40(1)5)).

275. These requirements apply only to respondent institutions outside the EEA and on a risk basis to those within the EEA.

276. ***Criterion 13.3*** – FIs are explicitly prohibited from establishing or continuing a correspondent relationship with shell banks or with FIs that knowingly allow shell banks to use their accounts (MLTFPA, §18(2)).

Weighting and Conclusion

277. FIs are required to take steps in line with R.13 for cross-border correspondent banking relationships. However, they apply only to respondent institutions outside the EEA and only on a risk-basis to those within the EEA. **R. 13 is rated PC.**

Recommendation 14 – Money or value transfer services

10. In the 3rd round MER, Estonia was rated LC on SRVI due to the lack of effective supervision of payment service providers. The 4th round MER of 2014 did not reassess Estonia's compliance with SRVI.

11. ***Criterion 14.1*** – In order to operate, legal persons that are MVTS providers (payment or e-money institutions) must hold a relevant activity licence. Natural persons cannot apply for a PSP/EMI licence (PIEIA, §§14(1)(3), 5(1) and 7(1)). Banks are not required to apply for an activity licence for providing payment services or issuing e-money (PIEIA, §14(5)(6)). PSPs and EMIs of third countries (non-EU) are required to apply for an authorisation in order to establish a branch or operate in Estonia. PSPs and EMIs of EEA member countries can found a branch or provide services in Estonia, subject to a notification submitted to the EFSA in advance (PIEIA, §§32(1), 35(1)). Universal postal service providers (UPSP) act as an MVTS when: (i) providing internal cash transfer services through the postal network based the Postal Act (§36) and (ii) carrying out money remittance activities under an agency contract (under the conditions specified at c.14.4). Historically and currently, there is only one UPSP – AS Eesti Post, which is owned by the government, with an activity licence issued by the Estonian Competition Authorities.

12. ***Criterion 14.2*** – In Estonia there is no specifically designated authority for detecting unlicensed MVTS activities. In circumstances when the unlicensed MVTS activity is carried out by an entity that is holding a licence (which does not entitle to provide MVTS services), without prior notification regarding the change of the business model, the respective licensing authority, i.e., EFSA or EFIU, would be responsible for detecting and sanctioning the illegal activities (FSAA, §§6(1)4[1]), 18(2)1), MLTFPA, §§74, 75, 97). The sanctioning powers are described under R.35 and can include issuing a precept requiring stopping certain activities or licence revocation.

13. When the unlicensed MVTS activity is carried out by an undertaking that is not a covered FI, the EFSA does not have powers to investigate or sanction such suspected undertakings. Instead, a criminal report shall be filed to the investigative authority or the Prosecutor's Office (CCP, §195(1)). The EFSA routinely searches social media and other public advertisements for businesses which operate in the regulated sector and are not appropriately licensed. It has

established a platform for reporting any violations by consumers or market participants[250] which serves as the main source of information for the identification of the entities operating illegally (complaints or whistleblowing). Carrying out economic activities without activity licence is a criminal offence pursuant to PC, §372 (see c.35.1).

14. ***Criterion 14.3*** – MVTS are subject to AML/CFT obligations. PSPs and EMIs are supervised for compliance with these obligations by the EFSA and the UPSP – by the EFIU (MLTFPA, §§6(2)2),3), 64(1)(2)).

15. ***Criterion 14.4*** – The agents of MVTS providers are required to be registered by the EFSA in order to operate legally in Estonia. The list of the agents is published on the EFSA website (PIEIA, §§59, 60). The necessary documents and the requirements for the agents are described by §§59(2) and 61 of the PIEIA.

278. ***Criterion 14.5*** – MVTS providers applying for an authorisation to provide its services through an agent, must submit to the EFSA a description of the internal control measures applied by the paying agent in order to comply with the MLTFPA (PIEIA, §59(2)3)). They also shall remain fully responsible for the due performance of the transferred duties by an agent, as well as for the compliance of the activities with the legal requirements (PIEIA, §62(5)). MVTS providers are required to establish the transfer procedure of its activities and duties to a paying agent by internal rules and the transfer shall not damage or decrease the capability of the MVTS providers to conduct effective internal control or exercise sufficient supervision over their internal activities, be contrary or affect the compliance with the conditions and obligations of the activity licence (PIEIA, §62(2)-(4)). However, there is no explicit requirement to include their agents in their AML/CFT programmes and monitor them for compliance with these programmes.

Weighting and Conclusion

279. MVTS providers are required to be licensed and supervised. However, there is no specifically designated authority for detecting unlicensed MVTS activities and no explicit requirement for MVTS providers to include agents in the AML/CFT programme or monitor their compliance. **R. 14 is rated LC.**

Recommendation 15 – New technologies

280. In the 4th round MER of 2014, Estonia was rated C on R.8.

281. ***Criterion 15.1*** – At the national level, in 2016 Estonia conducted analysis of ML/TF risks related to remote identification of customers; in 2021 the NRA analysed the ML/TF risks related to 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. Nevertheless, those assessments are not always accompanied with in-depth analysis.

282. 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)).

283. ***Criterion 15.2*** – (a) The covered FIs are required to undertake the risk assessment of

[250] www.minuraha.ee

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)). There is, nevertheless, no explicit requirement to undertake a risk assessment *prior to* the launch or use of such products, practices and technologies.

284. At the same time 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, use new or updated sales channels, which might suggest a prior risk assessment.

285. (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)).

286. ***Criterion 15.3*** – (a) In Estonia, the ML/TF risks related to the VA activities and VASPs were assessed within the scope of the NRA of 2021, sectorial risk assessment of the EFSA from 2021, and the EFIU – from 2020 and 2022.

287. 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 though 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 acknowledged that the available quantitative and qualitative data did not allow for the establishing of patterns, the profile of criminals or suspicious activities related to VASPs in Estonia (see also c.1.1).

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

289. 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 cooperation requests including the MLAs. 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)[251], nominal board member and shareholder (nearly 75% have a CSP among associated persons)[252], a small number of local employees (15 largest VASPs had a total of 27 employees in Estonia)[253].

[251] The SRA related to VASP sector, p.5 and 19
[252] The SRA related to VASP sector, p.19
[253] The SRA related to VASP sector, p.20

290. (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).

291. (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).

292. ***Criterion 15.4*** – (a) The definition of VASPs as amended in Mach 2022 covers all five activities as defined by the FATF (MLTFPA, §3(9^1)(10^3). VASPs are required to be licensed, and the EFIU is the competent authority (MLTFPA, §70(1)4), §71). An FI which is operating on the basis of a licence/authorisation granted by the EFSA need not to obtain a separate licence/ authorisation for providing VA services (MLTFPA, §70(2)). Nevertheless, the licencing regime of the FIs under the EFSA's competence, based on the sectoral legislation, does not permit performing VASP activities.

293. (i) The licensing requirement for legal person providing VASP services extends to the ones that have the registered seat, the seat of the management board and place of business is in Estonia, or the branch that is registered in the Business Register (BR) and the place of business and the seat of the head is in Estonia (MLTFPA, §72(1)4)).

294. (ii) The same provisions are applicable to the VASPs which are natural persons, since the term undertaking as defined in the legislation encompasses both, the natural and legal persons (General Part of the Economic Activities Code Act, §5(1), MLTFPA, §72(1)4)).

295. (b) The regulatory measures for VASPs are similar to those for the FIs that are under the competence of the EFIU. Those requirements are applicable for both legal and natural persons. The fit and proper assessment requires that the applicant, including the owner, BO and the members of the management body: (i) does not have any unspent conviction for a criminal offence against the authority of the state, offence related to ML or other intentionally committed criminal offence; (ii) has a proper business reputation, this extends also to associates with criminals (MLTFPA, §72(1)1),11). The detailed analysis on business reputation requirements is provided under c.26.3. Any subsequent appointment or change in the circumstances of a member of a governing body, owner, BO, or procurator is subject to a prior notification and approval by the EFIU, with an obligation to resubmit all the required documents (MLTFPA, §§70(3), 73, 74). The EFIU can also revoke an authorisation when the grounds which served for granting authorisation are no longer compliant (MLTFPA, §75(4)).

296. ***Criterion 15.5*** – In Estonia there is no specifically designated authority for detecting unlicensed VASP activities. In the circumstances when the unlicensed VASP activity is carries 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, BA or CN are those responsible for detection and sanction (FSAA, §6(1)4^1) and 18(2)1), MLTFPA, §§74, 75, 97; BAA, §19, §82^1; NA, §12, §17(2)). The respective sanctioning powers can be imposed in those circumstances (see R.35).

297. In order to detect the 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.

298. 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 activity licence is a criminal offence pursuant to PC, §372 (see c.35.1).

299. ***Criterion 15.6*** – (a) The EFIU is the designated supervisory authority VASPs and for ensuring compliance with the AML/CFT framework (MLTFPA, §64(1)). The EFSA is acting 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)). 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). However, it is not clear how the RBA models of the EFSA and the EFIU take into account the degree of discretion allowed to the covered FIs under the risk-based approach (see c.26.5). 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) 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).

300. ***Criterion 15.7*** – There are no VASP specific guidelines established in Estonia. Nevertheless, the EFIU had issued three guidelines that reflect on the characteristics of reports, the reporting obligation and on the management of risks relating to ML/TF and application of due diligence issued in 2019 and 2022 respectively. In addition, the EFIU had provided the VASPs with a sector specific feedback for years 2020 and 2021. There is, however, need for further guidance of sector specific typologies, in particular in respect to TF. This is especially important considering the materiality of the sector and a high level of TF risks in the sector.

301. ***Criterion 15.8*** – (a) The sanctions available for FIs apply equally to VASPs (the shortcomings under c.35.1 apply).

302. (b) 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 to both natural and legal persons,

thus being applicable to the directors and senior management of the VASPs. (see c.35.2).

303. ***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 are subject to the following qualifications.

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

305. (b) (i) and (ii) In relation to transactions of exchange or transfer of virtual currency, the VASPs are required to collect the information regarding the originator: the name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, the national identity number, date and place of birth and address (for legal persons – person's registry code or, in case of absence, the relevant identified in the country if its seat) (MLTFPA, §25 (2^4)). VASPs are also required to collect, with respect to the virtual currency or to the recipient of the transfer, the particulars of the transaction's unique identifier, and the beneficiary account number, where such an account is used to process the transaction. The unique identifier of a transaction must allow the transaction to be followed from its initiator to the recipient of the transfer. (MLTFPA, §25(2^5), (2^6)). There is no express requirement to obtain and hold the information regarding the name of the beneficiary. The mentioned information must be transmitted without delay to the recipient's VASP, together with transmission of the set of payment instructions to the recipient's VASP or to the recipient's credit or financial institution (MLTFPA, §25(2^7). There is no express requirement for the originator and beneficiary VASPs to make available this information, on request, to appropriate authorities.

306. (iii) When the beneficiary VASP is unable to receive or process the data, the originating VASP is required to ensure the monitoring of the transaction in real time and risk analysis in respect of each transaction. This obligation of the originating VASP is also applicable in the case of unhosted wallets (MLTFPA, §25(2^8). There is no requirement for the beneficiary VASP to perform post-event or real time monitoring in case of transfers which lack required originator or beneficiary information. Likewise, the beneficiary VASPs are not required to have risk-based policies and procedures in order to determine whether to reject or suspend a VC transfer and take appropriate follow-up up actions. TFS obligations apply to VASPs in the same manner as for the covered FIs.

307. (iv) There are no legal provisions to ensure that the same obligations apply to FIs when sending or receiving virtual assets transfers on behalf of a customer. The authorities suggested that such obligation would be covered by the provisions of the EU Regulation 2015/847. Nevertheless, its scope is limited to transfer of funds.

308. ***Criterion 15.10*** – UNSCRs 1267/1989, 1988 and 1373 are implemented in the EU by a number of EU regulations[254], which are directly applicable in Estonia, as per general EU law principles. *At the national level*, all regulatory measures apply identically to TF- and PF-related TFS. The EFIU shall immediately publish or make available on its website information regarding the imposition or amendments regarding designated persons and entities (ISA, §16(1)). There are no guidelines provided to VASPs on their obligation to take action under the freezing mechanism. When VASPs apply financial sanctions, they shall immediately inform about this the EFIU. This includes also intended transactions (ISA, §21(1)). The Sanctions applicable to VASPs for non-compliance with the obligations under R.7 are identical to the ones that apply to covered

[254] Regulations 881/2002 (UNSCR 1267/1989), 753/2011 (UNSCR 1988) and 2580/2001 (UNSCR 1373).

FIs and the deficiencies as per c.7.3, especially concerning the lack of sanctions for non-compliance with the freezing obligation, apply.

309. ***Criterion 15.11***– The international cooperation 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 apply (see c.37.6). Both supervisory authorities have a right to exchange information and cooperate with their counterpart authorities of other countries based on the duties provided by the MLTFPA (§64(6)). In addition, the EFIU is empowered to engage with the foreign FIU or a LEA with the purposes of ensuring implementation of the TFS by VASPs (ISA, §34)4-5)).

Weighting and Conclusion

310. Estonia conducts the risk assessment of new technology and services when launching the products to a large extent. It has a regulatory framework for VASPs and has conducted an ML/TF risk assessment. 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. However, although the licencing regime for FIs applied by the EFSA pursuant to the sectoral legislation does not permit performing VASP activities, they are entitled to provide VA related services. Implementation of AML/CFT obligations has moderate shortcomings due to the applicable deficiencies identified under R.10-21 and those regarding the VA transfers. Although subject to a broad range of sanctions, the regime for imposing financial penalties for AML/CFT and TFS violations pursuant to the misdemeanour proceedings is not considered sufficiently effective and dissuasive and there are no sanctions for non-compliance with the freezing obligation. There are also moderate shortcomings identified with respect to provided guidelines. Due to the materiality and high level of ML/TF posed by the VASP sector, these deficiencies are heavily weighted by the AT. **R. 15 is rated PC.**

Recommendation 16 – Wire transfers

311. In the 3rd round MER, Estonia was rated LC on former SR.VII due the lack of proper monitoring of Regulation (EC) 1781/2006 which was aimed to cover the requirements of SR.VII (effectiveness issue). The 4th round MER of 2014 did not reassess Estonia's compliance with former SR.VII.

312. Financial institutions are required to comply with the provisions of Regulation (EU) 2015/847 on information accompanying transfers of funds, which repealed Regulation (EC) 1781/2006 and is directly applicable in Estonia since 2017. Within the meaning of the Regulation (EU) 2015/847, it should be noted for Estonia that domestic wire transfers refer to transfers within the borders of the EU, while cross-border wire transfers represent transfers made to and from third countries. For consistency reasons, the analysis below uses the terminology of the FATF Recommendation interchangeably with that of the EU Regulation.

313. ***Criterion 16.1*** - (a) All cross-border wire transfers exceeding EUR 1 000 (so not covering transfers equal to EUR 1 000 in line with the standard) shall be accompanied by the following information on the payer i.e. the originator: (i) the name of the payer; (ii) the payer's payment account number; and (iii) the payer's address, official personal document number, customer identification number, or date and place of birth. In case of a wire transfer not made from a payment account, the PSP of the payer is required to ensure that the transfer is accompanied by a unique transaction identifier (Art.4(1)(3)). The PSP of the payer has the obligation to always verify the accuracy of the payer information on the basis of documents, data or information

obtained from a reliable and independent source before transferring funds (Art.4(4)).

314. (b) All cross-border wire transfers exceeding EUR 1 000 (so not covering transfers equal to EUR 1 000 in line with the standard) shall be accompanied by the by the following information on the payee i.e., beneficiary: (i) the name of the payee; and (ii) the payee's payment account number. In case of a wire transfer not made to a payment account, the PSP of the payer shall ensure that the transfer is accompanied by a unique transaction identifier (Art.4(1)(3)).

315. ***Criterion 16.2*** - The criterion on batch files transfer from a single originator where the PSPs of the payees are established outside the EU is implemented through Art. 6(1) with relevant references to Art. 4 for required and accurate originator information, as well as for required beneficiary information referred to under c.16.1, including the originator's account number or unique transaction identifier.

316. ***Criterion 16.3 -*** (a) and (b) Cross-border wire transfer not exceeding EUR 1 000 (and that does not appear to be linked to other transfers of funds which together exceed EUR 1 000) must be accompanied by at least: (i) the names of the payer and of the payee; and (ii) the payment account numbers of the payer and of the payee or, where Article 4 (3) applies, the unique transaction identifier (Art.6(2)).

317. ***Criterion 16.4*** - With regard to cross-border transfers not exceeding EUR 1 000, provided that they are not linked to other transfers of funds that cumulatively exceed EUR 1 000, the PSP of the payer need not verify the information on the originator referred to in c. 16.3 unless, inter alia, it has reasonable grounds for suspecting ML or TF (Art.6(2)).

318. ***Criterion 16.5 and Criterion 16.6*** - Wire transfers within the EU are considered domestic transfers for the purposes of R.16, which is consistent with the FATF standards. Domestic wire transfers shall be accompanied by at least the payment account number of both the payer and the payee or the unique transaction identifier (Art.5(1)). The PSP of the payer shall, within three working days of receiving a request for information from the PSP of the payee or from the intermediary PSP, make available the requested information set out under c.16.1 or c.16.3 (Art.5(2)). The PSP of the payer is also required to respond fully and without delay to enquiries from competent AML/CFT authorities (Art.14).

319. ***Criterion 16.7*** - The required information on the originator and the beneficiary must be retained by the PSP of the payer for a period of five years (Art.16(1)). Upon expiry of this retention period, personal data is to be deleted, unless provided for otherwise by national law. The further retention period shall not exceed five years (Art.16(2)). Pursuant to §47(7) of the MLTFPA, on the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of ML or TF may be retained for a longer period, but not for more than five years after the expiry of the first-time limit.

320. ***Criterion 16.8*** - The PSP of the payer is prohibited from executing a wire transfer before ensuring full compliance with its obligations concerning the information accompanying transfers of funds (Art.4(6)).

Intermediary FIs

321. ***Criterion 16.9*** - Art. 10 requires that intermediary PSPs to ensure that all the information received on the originator and the beneficiary, that accompanies a transfer of funds, is retained with the transfer.

322. ***Criterion 16.10*** - Regulation (EU) 2015/847 does not provide for the exemption specified

in this criterion regarding technical limitations preventing appropriate implementation of the requirements on domestic wire transfers. Pursuant to §59 of the ESAs' Joint Guidelines[255], the intermediary PSPs are required to use only payment or messaging systems that permit the onward transfer of all information on the originator or the beneficiary. Where this is not possible, including due to technical limitations, the intermediary PSPs should put in place alternative mechanisms to pass on relevant information to the PSP of the beneficiary.[256]

323. ***Criterion 16.11*** - Art. 11 requires that intermediary PSPs implement effective procedures including, where appropriate, ex-post or real time monitoring, in order to detect whether the required originator or beneficiary information in a transfer of funds is missing.

324. ***Criterion 16.12*** - The intermediary PSP is required to have effective risk-based procedures for: (i) determining whether to execute, reject or suspend a transfer of funds lacking the required information on the payer or the payee; and (ii) taking the appropriate follow-up actions (Art.12(1)). These procedures should be proportionate to the nature, size and complexity of the intermediary PSP's business, and commensurate with the ML/TF risk to which the intermediary PSP is exposed (§18 of the ESAs' Joint Guidelines). In case of repeated failures, the intermediary PSP shall take appropriate steps, which may initially include the issuing of warnings and setting of deadlines, and if the errors continue, it may begin either rejecting any future transfers of funds from that PSP or restricting or terminating its business relationship with that PSP. The intermediary PSP shall report that failure, and the steps taken, to the competent supervisory authority (Art.12(2)).

Beneficiary FIs

325. ***Criterion 16.13*** - The PSP of the payee shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer or the payee is missing in a cross-border wire transfer (Art.7(2)).

326. ***Criterion 16.14 -*** In case of wire transfers exceeding EUR 1 000, the PSP of the payee must verify the accuracy of the information on the payee on the basis of documents, data or information obtained from a reliable and independent source before crediting the payee's payment account or making funds otherwise available to the payee (Art.7(3)). The information on the payee must be retained by the PSP of the payee for 5 years (Art.16). Transfers of exactly EUR 1 000 are not covered - contrary to the FATF Standards.

327. ***Criterion 16.15*** - Art. 8 requires that the PSP of the payee shall implement effective risk-based procedures for: (i) determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information; and (ii) taking the appropriate follow-up action. The same steps and reporting obligations described under c.16.12 also apply.

MVTS operators

328. ***Criterion 16.16*** - The Regulation (EU) 2015/847 is binding for all MVTS providers and applies to the transfer of funds, in any currency, which are sent or received by an ordering, intermediary or beneficiary PSP established in the EU (Art.2(1)). The term "payment service providers" comprises the categories of PSP referred to in Art.1(1) of Directive (EU) 2015/2366

[255] Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information (No. JC/GL/2017/16 of 16.01.2018).
[256] EFSA complies with the Joint Guidelines as of 01.02.2018.

which includes money or value transfer services (Art.3(5)).

329. ***Criterion 16.17*** **-** (a) The PSP shall take into account missing information or incomplete information on the originator or the beneficiary in order to determine whether a suspicious report is to be filed in relation to the transfer of funds, or any related transaction (Art.13). The assessment of the suspicions shall take into account any criteria set out in the EU law, national legislation and own internal AML/CFT policies and procedures (§44 of the ESAs' Joint Guidelines). The PSP is required, when considering whether or not a transfer of funds raises suspicion, to take a holistic view of all ML/TF risk factors associated with the transfer of funds to the extent these are known, with a particular attention to transfers of funds that are likely to present a higher risk of ML/TF (§44 of the ESAs' Joint Guidelines).

330. (b) Regulation (EU) 2015/847 does not require a STR to be filed in any country affected by the suspicious wire transfer. However, given the principle of territoriality of AML/CFT, when a PSP, established in several countries, performs a wire transfer between two of its entities, and the transfer proves to be suspicious, it may be required to submit a STR to the FIU in each of these countries pursuant to their respective domestic laws. EU Directive 2015/849 requires compliance officers to file a STR with the FIU of the MS in whose territory the obliged entity having suspicion is established. Art. 50(1) of the MLTFPA requires that a suspicious activity report is to be submitted to the FIU of the contracting state of the EEA on whose territory the obliged entity has been established.

Implementation of Targeted Financial Sanctions

331. ***Criterion 16.18*** - FIs conducting wire transfers are subject to the requirements of the ISA, which gives effect to UNSCRs 1267, 1373, and successor resolutions (ISA, §20(1)2)).

Weighting and Conclusion

332. **R.16 is rated C.**

Recommendation 17 – Reliance on third parties

333. In the 3rd round MER, Estonia was rated LC on former R.9. The assessment identified technical deficiencies related to the lack of clear requirements for the REs to ensure that timey reproduction of the necessary documentation from third parties is possible; lack of guidance on which countries can be considered as having requirements equal to those provided in the MLTFPA; the FIs relying on third parties did not have the ultimate responsibility for the CDD measures applied by the third parties. The 4th round MER of 2014 did not reassess Estonia's compliance with former R.9.

334. ***Criterion 17.1*** – Covered FIs are permitted to rely, for partial or full performance of one or several CDD duties established under §20(1) of the MLTFPA, on data and documents gathered by another person (MLTFPA, §24(1)). The list of CDD measures under §20(1) that can be performed by other persons includes the "the monitoring of a business relationship", which is outside the FATF standard referring only to the elements (a)-(c) of the CDD measures. The authorities have suggested the reference to "all CDD measures", including monitoring, is a consequence of mistranslating the Estonian version into English. Nevertheless, the reference in the original language is still made to "seaduse § 20 lõikes 1", i.e., §20(1), which was introduced by the 2020 amendments of the MLTFPA[257]. The AML/CFT Advisory Guidelines of the EFSA details to a certain

[257] https://www.riigiteataja.ee/akt/112032022019

extent the previous obligations of the MLTFPA (§20(1)1)-4)), before the 2020 amendments, referring to two elements of the CDD measures which can be subject to third-party reliance, i.e., the identification of the client, including PEPs and of the BO (§4.8.2.2), except for the possibility to rely for understanding and obtaining information on the proposed and the intended nature of the business relationship (which correspond to the obligation under §20(1)4) of the MLTFPA).

335. The MLTFPA does not define the term "another person" that can be relied upon. From the provisions of §24(3) it appears that the "other person" who is relied on is required to comply and actually does comply with requirements equal to those established by the Directive (EU) 2015/849, including CDD and record-keeping requirements and is under regulatory enforcement regarding compliance with the requirements or "is prepared to be under regulatory enforcement" regarding the compliance with the requirements. Thus, this does not appear to be consistent with the definition of "third party" in the FATF Standards (IN to R.17), which is limited to FIs and DNFBPs that are "regulated, supervised and monitored".

336. The ultimate responsibility for applying the required CDD measures remains with the relying FI (MLTFPA, §24(7)).

337. (a) Covered FIs are obliged to obtain (gather) the necessary information concerning the elements (a)-(c) of the CDD measures. However, there is no specific requirement to obtain "immediately" such information (MLTFPA, §24(1)1)).

338. (b) FIs are required to ensure that, when necessary, all data and documents are obtained without delay, whereby they relied on the information gathered by another person (MLTFPA, §24(1)2)).

339. (c) as described above, §23(3) allows for the reliance on another person which is only "prepared to be" under regulatory enforcement regarding compliance with the CDD and record-keeping requirements.

340. ***Criterion 17.2*** – FIs are not allowed to rely on third parties established in high-risk third countries (MLTFPA, §24(6)). This is limited to the jurisdiction outside the EU/EEA area, as listed by the Regulation (EU) 2016/1674 and does not fully satisfy the requirement to regard the information on the level of country risk. There does not appear to be a list maintained by the Estonian authorities which would include jurisdictions posing a higher ML/TF risk based on its own NRA.

341. ***Criterion 17.3*** – FIs are allowed to rely on a person belonging to the same group, but only on those established in a country which applies equal requirements to those of the EU Directive 2015/849.

342. (a) These include, *inter alia* the CDD measures, identification of PEPs and record keeping obligations (R.10 and R. 12). There is no specific reference to the AML/CFT programmes, although this can be inferred from the requirements of the EU Directive and from the obligation to implement group-wide programmes against ML/TF (R.18) (MLTFPA, §24(5) and §15).

343. (b) A group-based supervision is required to be exercised over the group (MLTFPA, §24(5)).

344. (c) When part of the same group, covered FIs are permitted to rely only on persons established in a country (both EU and non-EU) where requirements equal to those of EU AML/CFT Directive apply (MLTFPA, §24(5)). The EFSA AML/CFT Guidelines prescribes that the risk appetite and risk assessment documents of an FI belonging to a group must consider the

respective documents and assessments of other members of the group and that the group-wide rules of procedures must cover a description of compensation mechanisms that would comply with the risks of the group and the risks of each group company[258] (§3.9). However, these requirements are not established by the MLTFPA, which provides for ML/TF risk mitigating measures only in relation to high risk third countries (outside EAA).

Weighting and Conclusion

345. There are measures in place for the use of regulated third parties. Nevertheless, the reliance is also permitted in the case of persons who are only *prepared to be under regulatory enforcement.* The elements of the CDD measures which can be performed by a third party include the monitoring obligation, contrary to the standard. Deficiencies exists stemming from the assumption that all EU member states apply adequate AML/CFT controls and are not high risk. **R. 17 is rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

346. In the 3rd round MER, Estonia was rated LC on both former R.15 and R.22. The 4th round MER of 2014 did not reassess Estonia's compliance with R.15 and R.22. The 3rd round MER noted that the FIs were not required to: have internal guidance concerning the detection of unusual and suspicious transactions, apply the AML/CFT measures to foreign branches and subsidiaries beyond CDD and record keeping, pay special attention to situations where the host country do not or insufficiently applies FATF standards, or to apply the highest standard when the minimum AML/CFT requirements of the home and host country differ; there were limited requirements for the FIs concerning the screening procedures of the new employees and AML/CFT trainings.

347. The introduction to R.10 lists the activities which are outside the scope of the MLTFPA.

348. ***Criterion 18.1***– Covered FIs are required to implement programmes against ML/TF, which must take into account the results of the NRA and individual ML/TF risks (MLTFPA, §§13, 14(1)). The internal rules of procedure and the internal control rules may be contained in a single or multiple documents and must be proportionate to the nature, size and level of complexity of the economic activities of the FI, and updated regularly (MLTFPA, §14(3)).

349. (a) The compliance management obligations include: (i) appointing a management board member (where the entity has more than one management board member), in charge of implementation of the AML/CFT obligations; (ii) appointing a compliance officer, who must meet the education, professional, experience and the impeccable reputation requirements. The appointment must be coordinated with the EFIU (MLTFPA, §14(1)(2)(5)).

350. (b) The internal control rules must set out, *inter alia,* the procedure for employee screening (MLTFPA, §14(3)).

351. (c) The covered FIs are required to ensure that the employees with AML/CFT competences are provided with initial and continuous training (MLTFPA, §14(6)).

352. (d) The internal control rules must include the procedure for the implementation of internal audit, which shall ensure the adherence to the AML/CFT obligations, and the internal rules and procedures established pursuant to the MLTFPA (MLTFPA, §14(1)(5)). The sectoral legislation further requires the covered FIs supervised by the EFSA, except for the investment

[258] The footnote 53 to §3.9.1 of the EFSA AML/CFT Guidelines makes reference to FIs part of the group, based in Estonia and outside Estonia.

firms, to have an independent audit function (CIA, §59(3); PEIA, §51(2); CCIA, §45(2); FMA, §349(1); IAA, §103(2); SMA, §83). A similar requirement is prescribed for the FIs under the EFIU supervision by the EFIU AML/CFT Guidelines (§3.5.4.1).

353. ***Criterion 18.2*** – An FI that is the parent undertaking of a group is required to apply group-wide rules of procedures and internal control rules (MLTFPA, §15(1)).

354. (a) This shall include group-wide procedure for exchanging information on AML/CFT (MLTFPA, §15(1)). As explained by the EFSA Explanatory AML/CFT Guidelines, this also covers the exchange of information related to CDD and management of ML/TF risks (§3.9.3.4).

355. (b) Within the group, the information on a suspicion reported to the EFIU has to be shared, unless the FI is otherwise instructed by the EFIU (MLTFPA, §15(5)). This shall also cover, as explained by the EFSA advisory Guidelines, the analysis of suspicious and unusual transactions, the related circumstances and the measures of keeping up to date with the applicable risks (§3.9.3.4).

356. (c) The group-wide procedures shall also establish rules for protection of personal data (MLTFPA, §15(1)). This shall include, as explained by the EFSA advisory Guidelines, procedures for ensuring the confidentiality and secrecy of transmitted data, to avoid, among others, situations of tipping-off, and restriction on the use of information transmitted in the group (§3.9.3.5).

357. ***Criterion 18.3*** – Covered FIs are required to ensure that their foreign branches and majority-owned subsidiaries comply with the requirements established under the MLTFPA, including the requirements for protection of personal data, to the extent permitted by the law of the third country, where the minimum requirements of the host third country are less strict than those established in Estonia. This does not apply to cases when the host country is an EU members state, which, e.g., did not implement effectively the provisions of the EU Directive 2015/849 and, therefore, has less strict requirements (MLTFPA, §15(2)).

358. In relation to third countries, the FIs must also ensure the application of additional risk mitigating measures and inform the home supervisory authority (MLTFPA, §15(3)(4)).

Weighting and Conclusion

359. FIs are required to develop and implement programs against ML/TF and to implement internal policies at the group level. However, the obligations established for dealing with host countries with less strict AML/CFT requirements do not apply to cases when the country is an EU members state. The audit function of the investment firms is not required to be independent. The shortcomings described under R.10 regarding the scope of application of the MLTFPA apply. **R. 18 is rated LC.**

Recommendation 19 – Higher-risk countries

360. In the 4th round MER of 2014, Estonia was rated PC with the former R.21 based on the following: (i) technical deficiency in relation to the application of the obligation to a customer or person from one of the stipulated countries; (ii) no clear requirement to examine the nature, purpose or background when discovering a transaction with no apparent economic or visible lawful involving higher risk countries; and (iii) no clear requirement to keep records of findings that do not lead to STR.

361. The following activities which are covered by the FATF definition of FIs are not subject to

the MLTFPA obligations: companies managing a mandatory pension fund and life insurance companies providing services related to mandatory funded pension insurance contracts within the meaning of Funded Pensions Act.

362. ***Criterion 19.1*** – The OEs shall apply EDD measures when natural or legal persons are from a high-risk third country or where their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country (MLTFPA, §36(2)3)). A high-risk third country is defined as a country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 (MLTFPA, §3(18)). Thus, the requirement to apply EDD measures is limited to the high-risk jurisdictions outside the EU/EEA area.

363. In addition, the EDD measures do not need to be applied to the branch of an OE established in a contracting state of the EEA or a majority-owned subsidiary seated in a high-risk third country, provided that the branch and the majority-owned subsidiary fully comply with the group-wide procedures and the OE assesses that the waiver to apply EDD measures does not entail major additional ML/TF risks (MLTFPA, §36(4)).

364. There is a gap which is mitigated through the combination of the following requirements for application of the risk – based AML/CFT measures. The OE should apply CDD measures determining the scope and the manner of their application on the basis of assessment of ML/TF risks related to a specific business relationship, an occasional transaction, operation or person (MLTFPA, §20(6)). When assessing the ML/TF risks the OE, among others considers the geographical risk. A range of factors may substantiate increased geographical risk, such as that: (i) according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems; (ii) according to credible sources, has significant levels of corruption or other criminal activity; (iii) is subject to sanctions, embargos or similar measures issued by, for example, the EU or the UN; (iv) that provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by the EU or UN (MLTFPA, §37(4)) .

365. ***Criterion 19.2*** **–** There are no legal provisions suggesting that the Estonian competent authorities should be able to apply countermeasures when this is called for by the FATF or independently, except for the requirement of EDD measures in the circumstances set out in c.19.1.

366. ***Criterion 19.3*** – After each FATF plenary, the EFSA circulates the two updated FATF lists of jurisdictions subject to a call for action and jurisdictions under increased monitoring to its supervised FIs. There is no indication that the EFIU does the same in relation to the FIs that it supervises. In addition, the NRA of Estonia should specify among others, countries or jurisdictions with regard to which covered financial institutions should apply EDD measures (MLTFPA, §11(1)2).

Weighting and Conclusion

367. There are moderate shortcomings in implementation of measures to higher risk countries. The FIs are required to apply the EDD measures towards countries listed by the EU, which is narrower than the FATF approach. No legal basis is provided for application of countermeasures by Estonia either when called upon by the FATF or independently. Sufficient measures to ensure FIs are advised about the countries with weak AML/CFT systems are in place only for FIs supervised by the EFSA. **R. 19 is rated PC**.

Recommendation 20 – Reporting of suspicious transaction

368. In the 4th round MER of 2014, Estonia was rated LC with the former R.13 and SR.IV. The AT noted that there was no explicit requirement to report suspicions on funds linked or related to terrorism, terrorist acts or by terrorist organisations. Estonia adopted a large variety type of reports to be filed by OEs: STRs, UTRs, UARs, TFR, and TR_UAR. These differ from the STRs by the threshold of the level of suspicion and do not require the suspension of the transaction.

369. The following activities which are covered by the FATF definition of FIs are not subject to the MLTFPA obligations: companies managing a mandatory pension fund and life insurance companies providing services related to mandatory funded pension insurance contracts within the meaning of Funded Pensions Act.

370. ***Criterion 20.1*** – When FIs identify activity or facts characteristics of which indicate the use or attempted use of the proceeds of crime, TF or associated offenses or suspects or knows that it is ML, TF or the commission of associated criminal offenses, they shall notify the EFIU immediately, but not later than two working days after the establishment of the activity, facts or suspicion (MLTFPA, §49(1)). This mechanism to file notifications is considered timely and is considered adequate in relation to known or suspected cases of ML, TF and predicate offenses. However, while the MLTFPA provides that FIs should submit a report when they know or suspect that funds are the proceeds of a criminal activity or are related to TF, it does not explicitly provide that FIs should submit a report when they have reasonable grounds to suspect that funds are the proceeds of crime or are TF-related.

371. The EFIU's "Guidelines on the characteristics of suspicious transactions" is aimed at providing instructions for the fulfilment of the reporting obligation set out in §49 of the MLTFPA. The document contains indicators for the reporting of, *inter alia*, suspicious transactions (STR), unusual transactions (UTR) and unusual activities (UAR). However, these indicators do not appear to compensate for the lack of obligation to report on the basis of having reasonable grounds to suspect.

372. Deficiencies in criminalisation of TF restrict the scope of the TF reporting requirement (see R.5).

373. ***Criterion 20.2*** –The requirements for notifying the FIU as set in c.20.1 apply to transaction, including when attempted (MLTFPA, §49(2)). There is no limitation of amount of transaction set in the legislation.

Weighting and Conclusion

374. Estonia implemented measure for reporting suspicious funds and transactions promptly, but important deficiencies remain with the reporting obligation and the coverage of TF activities. **R.20 is rated PC.**

Recommendation 21 – Tipping-off and confidentiality

375. In the 4th round MER of 2014, Estonia was rated C on R.14.

376. The following activities which are covered by the FATF definition of FIs are not subject to the MLTFPA obligations: companies managing a mandatory pension fund and life insurance

companies providing services related to mandatory funded pension insurance contracts within the meaning of Funded Pensions Act.

377. ***Criterion 21.1*** – "[T]he performance of the duty to report arising from § 49 of this Act and submission of information by the obliged entity is not deemed breach of the confidentiality requirement arising from law or contract and the statutory or contractual liability for the disclosure of the information is not applied to the person who performed the duty to report. An agreement derogating from this provision is void." (MLTFPA, §52).

378. Moreover, according to Section 52(1) of the MLTFPA, the obliged entity, its employee, representative and the person who acted on its behalf is not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing an official operation or in the provision of an official service … in connection with the performance of the duty to report provided for in § 49 of this Act in good faith. In the scope of Estonian legal terminology, the term "representative" is meant to cover directors and officers of a FI.

379. ***Criterion 21.2*** – The MLTFPA sets out the principle that FIs, their structural units, members of management bodies and employees are prohibited from disclosing the fact that a report is planned to be submitted, or is submitted, to the FIU and from disclosing the issuance of a compliance notice by the FIU or the commencement of criminal proceedings (MLTFPA, §51(1)). However, there is an exception to this principle that R.21 does not provide for. Specifically, after the FI has complied with the FIU's compliance notice, the FI may inform the interested person that the FIU has restricted the use of their account, essentially tipping them off. The Authorities justify this exception on account of the relatively long duration of the restriction (at least 30 days, up to a maximum of 90 days). This is exception is not assessed to be a minor deficiency. Moreover, the prohibition cited in MLTFPA (§51) refers to reports, without making any reference to related information.

380. The provisions on tipping off do not inhibit information sharing under R.18 (MLTFPA, §51(2)).

Weighting and Conclusion

381. Estonia has provisions on confidentiality of information and restricting tipping-off, but there are deficiencies related to the scope of protection from liability and disclosing information to the EFIU. **R.21 is rated PC.**

Recommendation 22 – DNFBPs: Customer due diligence

382. In the 4th round MER of 2014, Estonia was rated PC on former R.12. The report noted the lack of clear requirements for determining whether the customer is acting on behalf of another person and no requirement to apply CDD to existing customers, as well as effectiveness issues in the implementation of the CDD measures (higher-risk customers, PEPs, RBA) applicable to all DNFBPs, and weakness in the implementation of CDD measures by real estate agents and DPMSs.

383. The following activities, which are covered by the FATF definition of DNFBPs, are not subject to the MLTFPA obligations: dealers involved in the purchase and sale of precious metals used or production, scientific or medical purposes.

384. ***Criterion 22.1*** – Covered DNFBPs are required to comply with the CDD obligations.

385. (a) Gambling operators are required to apply CDD measures when a customer receives a

payment of winnings, and/or placing a bet of 2000 euros (or currency equivalent), regardless of whether the payment is performed as a single operation or several related payments over a period of one month (MLTFPA, §19(3)).

386. (b) §2(1)4) of the MLTFPA includes the activities of any person that mediate the purchase or sale of an immovable property.

387. (c) CDD measures shall be performed by DPMSs - persons buying-in or wholesale of precious metals, precious metal articles precious stones, by way of business (MLTFPA, §2(1)6)). As explained in the introduction to this recommendation, the CDD obligations are not applicable to dealers involved in the purchase and sale of precious metals used for production, scientific or medical purposes.

388. (d) Notaries, lawyers and providers of other legal services are subject to CDD obligations when they act in the name and on account of a customer in a financial or real estate transaction, as well as when the mentioned persons guide the planning, making of a transaction, performs the transaction/ service in relation to: (i) the purchase or sale of an immovable property, business or shares of a company; (ii) management of client money, securities or other property; (iii) opening or management of payment, deposit or securities accounts; (iv) acquisition of funds required for the foundation, operation or management of a company; (v) the foundation, operation or management of a trust, company, foundation or legal arrangements (MLTFPA, §2(2)). Certified auditors, upon provision of accounting services, providers of accounting or tax advise services are also subject to CDD obligations (MLTFPA, §2(1)7), 8)).

389. (e) Trust and company service providers are required to apply CDD measures when providing at least one of the following services: (i) foundation of a company or another legal person, including operations and steps related to transfer of shareholding; (ii) acting as an officer or management board member in a company, as a partner in a general partnership, or in such a position in another legal person, as well as arrangement of assumption of such position by another person; (iii) enabling use of the address of the seat or place of business; (iv) acting as a trustee or a representative of a civil law partnership, community or legal arrangement, or the appointment of another person to such position; (v) acting as a representative of a shareholder of a public limited company or arrangement of the representation of a shareholder by another person (MLTFPA, §2(1)9), §8).

390. ***Criterion 22.2*** – The MLTFPA applies to businesses listed under C.22.1. See R.11 for a description of record-keeping requirements.

391. ***Criterion 22.3*** – See R.12 for a detailed description of measures taken by Estonia to comply with the PEPs requirements and the identified gaps.

392. ***Criterion 22.4 –*** See R.15 for a detailed description of measures taken by Estonia to comply with the new technologies requirements and the identified gaps.

393. ***Criterion 22.5 –*** See R.17 for a detailed description of measures taken by Estonia to comply with the reliance on 3rd parties requirements and the identified gaps

Weighting and Conclusion

394. DNFBPs are subject to the same CDD obligations as FIs, as required by R.10 However, not all activities covered by the FATF definition of DNFBPs are subject to AML/CFT obligations (dealers involved in the purchase and sale of precious metals used or production, scientific or

medical purposes). The shortcomings identified in relation to FIs under R.10, 12, 15 and 17 are also relevant for DNFBPs. **R. 22 is rated LC.**

Recommendation 23 – DNFBPs: Other measures

395. In the 4th round MER of 2014, Estonia was rated PC on former R.16. The report noted the following technical shortcoming: no requirement to report suspicions on funds related to TF, as well as effectiveness issues related to the initial postponement decision and underreporting by certain DNFBPs.

396. R.22 lists the activities to which the MLTFPA does not apply.

397. ***Criterion 23.1*** – Covered DNFBPs, as obliged entities, are required to report suspicious transactions based on the same provisions of the MLTFPA as FIs (MLTFPA, §49(1)). §49(5) of the MLTFPA contains a legal privilege-based exemption to the reporting obligation by lawyers and other legal professionals, notaries and accountants where they are providing legal advice or representing the client in litigation. Dealers involved in the purchase and sale of precious metals used or production, scientific or medical purposes are not obliged entities and so they are not subject to the obligation to report.

398. ***Criterion 23.2*** – Requirements described in relation to FIs under R.18.1 are equally applicable to DNFBPs. Additionally, the covered DNFBPs may apply to the competent supervisory authority for partial or full release from the obligation to prepare the documents on the rules of procedure and internal control rules (MLTFPA, §14(7)).

399. ***Criterion 23.3*** – Requirements and shortcomings described in relation to FIs under R.19 are equally applicable to DNFBPs.

400. ***Criterion 23.4*** – Requirements and shortcomings described in relation to FIs under R.21 are equally applicable to DNFBPs.

Weighting and Conclusion

401. DNFBPs are required to comply with the requirements of R.20. However, the shortcomings underlined under R.22 with regard to the scope of application of the MLTFPA are also relevant here. Covered DNFBPs are subject to the requirements of R.18, as the FIs, although they may apply for an exception from the internal control requirements. The shortcomings identified under R.19 and R.21 are equally applicable to DNFBPs **R. 23 is rated PC**.

Recommendation 24 – Transparency and beneficial ownership of legal persons

402. In the 4th round MER of 2014, Estonia was rated PC with former R.33. The assessment identified technical deficiencies related to the limited control over the obligations of legal persons to submit updated information on ownership and control to the register; lack of supervision over maintenance of share and shareholder registers by limited companies; gaps in the legal framework, which did not ensure that information held in the CR was adequate, accurate and timely; and doubts regarding the ability of the competent authorities to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons.

403. ***Criterion 24.1*** – The mechanisms stipulated under this criterion are provided in the General Part of the Civil Code Act (GPCCA), the COC, the Non-Profit Associations Act (NPAA), the FA, the MLTFPA and other applicable legislation, as follows:

404. *a) Types, forms and features of legal persons* – The COC provides the regulation of different types, forms and basic features of legal persons in private law[259]. COC (§2) defines five forms of business entities – general partnerships, limited partnerships, public limited companies, private limited companies and commercial associations. Types of non-business entities, i.e., non-profit associations and foundations[260], are defined under NPAA (§2) and FA (§2). The passive legal capacity of business and non-business entities commences as of their entry in, and terminates as of their deletion from, the CR and the Register of Non-Profit Associations and Foundations (NPAR), respectively[261].

405. According to COC (§22) and NPAA (§75), the registration department of the Tartu County Court shall maintain the CR of the enterprises of sole proprietorships, companies and branches of foreign companies located in Estonia, as well as the NPAR, along with a number of other registers/databases available in the country[262]. The registers of business and non-business entities are publicly available on the web portal e-Business Register.

406. *(b) Process for creation of legal persons and obtaining basic and beneficial ownership information* – The processes for creation of legal persons, as well as for obtaining basic ownership information are provided in the COC for business entities, and in the NPAA and the FA for non-business entities (see further details in the analysis for c.24.3). MLTFPA (§76) states that a legal person in private law gathers and retains data on its BO, including information on the owner's right of ownership or methods of exercising control. The data of the BO are kept by the management board of the private legal person in the Beneficial Ownership Information Database (BOID). To achieve this, the same section of the law requires shareholders or members of a private legal person to provide the management board of the legal person with all information known to them about the BO, including information on its right of ownership or manners of exercising control. MLTFPA (§ 76^2) regulates the establishment of the BOID, which is substance-wise separate from the CR and the NPAR. However, the data from the BOID is accessible via the e-Business Register.

407. The duty to collect and retain BO information does not apply to: 1) apartment and building associations regulated by relevant acts; 2) companies listed on a regulated market; and 3) foundations established exclusively for keeping or accumulating the property of the beneficiaries or the circle of beneficiaries specified in the articles of association. With regard to the arrangements providing for compliance of the classes of non-business entities specified in points 1 and 3, the authorities advise that:

- Activities of apartment and building associations are regulated by a specific act, which sets limitations to such activities, as well as to the possible members of associations, which can

[259] The term *"legal person in private law"* is defined in the GPCCA (§25) as the legal person founded in private interests and in accordance with the respective laws governing their activities, particularly COC for companies (i.e. general partnerships, limited partnerships, private limited companies, public limited companies and commercial associations), NPAA for non-profit associations, and FA for foundations.

[260] The key difference between a non-profit association and a foundation is that the latter *"is a legal person in private law which has no members and which is established to administer and use assets to achieve the objectives specified in its articles of association"* (FA, §2).

[261] Types, forms and features, as well as processes for creation of companies under EU law, i.e. European public limited liability companies, European cooperative societies and European economic interest groupings, are provided in the respective EU regulations (2157/2001, 1435/2003 and 2137/85) and Estonian implementing acts, which stipulate that these entities will be entered into the register based on the provisions applicable to, respectively, public limited companies, commercial associations, and general partnerships.

[262] Such as the e-Notary system, the e-Land Register, the information system of courts, the Probation Supervision Register, the Prisoners Register, the Criminal Records Database, the e-File, the electronic State Gazette, etc.

only be the owners of immovable property that make up the building, i.e., information on the beneficiaries is already publicly available via the Land Register[263]. Data in the Land Register is presumed correct according to the Law of Property Act (§56(1)), and it is verified by notaries. If the property belongs to a legal person, the BOs are available via BOID.

- According to FA (§8(1(5)), the articles of association shall establish the set of beneficiaries, except if all persons who are entitled to receive disbursements pursuant to the objectives of the foundation are beneficiaries. According to FA (§ 9) a beneficiary is a person to whom disbursements from the assets of the foundation may be made pursuant to the articles of association of the foundation. If a set of beneficiaries is not determined by the articles of association, all persons who are entitled to receive disbursements pursuant to the objectives of the foundation shall be deemed to be beneficiaries. The authorities advise that while BO information on such foundations is not provided to the BOID, it is available in the same interface via the NPAR.

408. ***Criterion 24.2*** – Chapter 4.2 of the NRA 2021 analyses the types of business entities in private law (i.e., general partnerships, limited partnerships, private limited companies, public limited companies and commercial associations) and assesses ML/TF risks pertaining to such legal persons. ML/TF risk exposure of non-business entities in private law (i.e., non-profit associations and foundations) is analysed and assessed in Chapter 8 of the NRA 2021. Nonetheless, due to the reasons set out under the analysis for R.1 (c.1.1), these analyses do not appear to provide a reliable assessment of the ML/TF risks associated with all types of legal persons created in the country.

409. ***Criterion 24.3*** – According to COC (§36), on each registered legal entity the CR shall maintain entries in three categories: 1) a registry card; 2) business files; and 3) registry files.

410. COC (§64) defines the contents of the registry card with the CR, which includes, *inter alia,* the entity's business name and registry code; residence or registered office and address; information on general partners/members of the management board; legal form or class of company; date of approval of the articles of association; agreements on the right of representation of general partners/members of the management board; information on limited partners; a notation concerning entry of the shares in the Estonian Central Register of Securities. For private and public limited companies, relevant provisions of COC require the CR to obtain and maintain articles of association (§144 and §250), basic regulating powers (§145 and §251), and list of directors (§145 and §251) of these business entities.

411. For general partnerships, COC (§84(4-5)) requires to enter in the CR names, personal identification codes or registry codes of the partners, as well as the partners authorised to represent the general partnership, and which of them are entitled to represent the general partnership jointly. General partnerships do not have articles of association, but a partnership agreement (COC, §82) that is not submitted to the CR. The same provisions apply to limited partnerships (COC §125(2)). According to Commercial Associations Act (CAA) §(7(1(2)) the articles of association of commercial association shall be appended to the petition for entry in the CR. CAA (§8(4- 5) require to submit to the CR the names and personal identification codes of the members of the management board and the members of the management board entitled to represent the association jointly.

[263] https://kinnistusraamat.rik.ee/Avaleht.aspx?lang=Eng

412. Similar arrangements for gathering and maintaining information on non-business legal entities are provided in the NPAA and the FA. According to NPAA (§89) and FA (§14), the registry card of a non-profit association or a foundation with the NPAR includes, *inter alia*, the entity's name and registry code; registered office and address; information on members of the management board; the right of representation of members of the management board; date of approval of the articles of association. For non-profit organisations, relevant provisions of NPAA require the NPAR to obtain and maintain articles of association (§8), basic regulating powers (§10 and §27) and identity of the members of management board (§10). According to FA (§11)1 (1)), articles of association shall be appended to the petition for entry in the NPAR. FA (§14(1(5),(8)) require to enter on the registry card of the foundation information on the members of the management board and the right of representation of the members of the management board, if such right differs from the general rule prescribed by FA.

413. COC (§28) and NPAA (§77) define that entries in the CR and in the NPAR are public. Everyone has the right to examine and obtain copies of the registry cards, the business files (in case of the CR) and the public files (in case of the NPAR). Both the CR and the NPAR are electronically kept databases, and the information on registry cards, business files and public files is accessible via e-Business Register[264].

414. ***Criterion 24.4*** – According to GPCCA (§26(2)), the passive legal capacity of a legal person in private law arises as of entry of the legal person in the register prescribed by law. This means that the basic information set out in c.24.3 should be without failure provided to the CR or NPAR of Estonia for business and non-business entities to obtain legal capacity upon registration. At that, according to GPCCA (§27(2)), some of the documents comprising basic information, i.e., the memorandum of association or foundation resolution of the legal person in private law are deemed to be valid after the entry of the legal person in the register, even if they have been adopted under circumstances rendering the said documents void, and they cannot be repealed after the legal person has been entered into the register.

415. Moreover, the COC (§122 for general partnerships, §219 for private limited companies, and §382 for public limited companies) and the NPAA (§54 for non-profit associations) provide for preservation of company documents[265] after the liquidation/ removal of the legal entity from the register by way of depositing such documents with liquidators, persons maintaining archives or "another trustworthy person". Similar provisions on the preservation of company documents for the other types of legal persons are provided as follows: for foundations – FA (§59); for commercial associations – COC (§94); for limited partnerships the provisions concerning general partnerships apply – COC (§125) 2); for public limited companies – COC (§382). These provisions only apply to the documents not submitted to the CR or the NPAR.

416. COC (§233) provides that the share register maintained by the registrar of the ECRS[266] shall comprise the following information on public companies: name, address and personal identification code or registry code of the shareholder; class and nominal value of the shares; and date of subscription and acquisition of the shares. According to Securities Register Maintenance

[264] https://ariregister.rik.ee/eng

[265] With their exact composition deriving from other provisions, such as the Accounting Act (§ 2 (2), § 7 (9), 11 (1), § 12); Value-Added Tax Act (§ 36 (1), (3), (4)); Taxation Act (§ 58); and Employment Contacts Act (§ 5 (5)).

[266] The ECRS is a legal person specified in Article 2(1)(1) or (2) of Regulation (EU) No909/2014 of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012.

Act (§2), the ECRS[267] registers the shares of public limited companies. The management board of the public limited company is obliged to ensure timely submission of accurate information provided by law to the ECRS.

417. Nonetheless, the regulations described above do not amount to a requirement for: 1) business and non-business entities – to maintain the basic information set out in c.24.3; and to ensure that such information is maintained within Estonia; 2) business entities – to maintain a register of their shareholders or members containing the number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights), at a location notified to the CR; and 3) non-business entities – to maintain a register of their members or founders, at a location notified to the NPAR.

418. ***Criterion 24.5***– COC (§33(7)), NPAA (§10(2)) and FA (§14(2)) define a general obligation of business and non-business entities to file an application with the CR or NPAR for amendment of registry information upon any changes in registered data (for business entities, also including in the case of appointment, removal or change of the right of representation of a member of the management board or a liquidator of the company, or on dissolution of the company). Other than this, there are no mechanisms, such as verification or monitoring tools, cross-checking and sample testing practices, or arrangements for reporting discrepancies to ensure that the information referred to in criteria 24.3 and 24.4 is accurate and updated on a timely basis.

419. ***Criterion 24.6*** – The primary mechanism ensuring availability of BO information in the country is provided under MLTFPA (§76) stating that legal persons in private law collect and retain data on their BOs, including information on their right of ownership or manners of exercising control. BO information obtained by the management board of the private legal person is kept in the BOID. To achieve this, the same section of the law requires shareholders or members of a private legal person to provide the management board of the legal person with all information known to them about the BO, including information on its right of ownership or manners of exercising control.

420. BO information to be filed with the BOID using the infrastructure of the e-Business Register comprises the following: for **companies and non-profit associations** – 1) the person's name, personal identification code and the country of its issuance (upon absence of a personal identification code, the date and place of birth), and the country of residence; and 2) nature of the beneficial interest held; and for **foundations** – in addition to the information required with regard to companies and non-profit associations, also 3) the list of beneficiaries within the meaning of the FA (§9[268]), which contains each beneficiary's name, personal identification code and the country of the personal identification code (upon absence of a personal identification code, the date and place of birth), and the country of residence, where such persons have been specified in the articles of association of the foundation.

---

[267] In addition, ECRS registers the following securities: 1) debt obligations issued by legal persons in public law (i.e. the Republic of Estonia, local authorities of Estonia and other legal persons in public law); 2) debt obligations issued by legal persons in private law, whose public offer prospectus is registered with the EFSA pursuant to the Securities Market Act; 3) units and shares of investment funds, which are admitted for trading on a regulated securities market or in a multilateral trading facility; 4) subscription rights for publicly issued or publicly offered shares and securities; 5) covered bonds issued by credit institutions upon additional authorization from the EFSA.

[268] Under this section , a beneficiary is defined as *"a person to whom disbursements from the assets of the foundation may be made pursuant to the articles of association of the foundation. If a set of beneficiaries is not determined by the articles of association, all persons who are entitled to receive disbursements pursuant to the objectives of the foundation shall be deemed to be beneficiaries"*.

421. Another mechanism to determine BO information is provided under MLTFPA (§20(2^1)) establishing that, where the obliged entity establishes a business relationship with a customer whose information on beneficial owners must, in accordance with the statutes of a EU Member State, be submitted to the state or be registered there, the obliged entity must obtain a relevant registration certificate or registry extract upon determination of BO information as part of the CDD process (this relates to cases when BO information is maintained in a centralised register of an EU Member State).

422. According to the MLTFPA (§20 (24)) entered into force on March 2022, a requirement has been introduced for OEs to notify to the registrar, within a reasonable time, discrepancies with the BO information published in the BOID, by attaching information or documents that show the differences. The latter, in turn, receives and maintains BO information filed by companies, notifies them about discrepancies of BO information as reported by obliged entities, proposes addressing such discrepancies within 10 working days by providing additional information and proof to the register, or changing the BO accordingly.

423. As to the disclosure requirements for listed companies, these are regulated under European Union directives and supervised by the national financial supervisory authority, i.e., by the EFSA in Estonia. Listing requirements follow EU standards and are intended for well-established companies. The transparency requirements ensure that beneficial ownership of listed companies is at all times clear.

424. ***Criterion 24.7*** – MLTFPA (77(5-6) provide the mechanism for updating BO information maintained with the BOID. In particular, whenever changes occur in the submitted data, companies, non-profit associations and foundations are required to submit new data not later than 30 days after learning of such changes. In case of no changes in BO information, they should certify the correctness of data upon submission of the annual report. The obligation to prepare and submit annual reports is established under COC for all undertakings (§32), for general partnerships (§97^1), for limited partnerships (§125(2)), for private limited companies (§179), for public limited companies (§334), as well as under NPAA (§36) and FA (§14).

425. As another instrument to ensure that BO information is accurate and up-to-date, MLTFPA (§79) defines that any person declared as the BO of any legal person has the right to request that the management board of the legal person corrects any incorrect data in the register. Where the management board of the legal person has without reason refused to comply with such request, the person indicated as the beneficial owner may demand that the legal person compensates for damage caused by making incorrect data public. The authorities advise that there is no practice of determining such damage, as the cases they are aware of have been solved before the court involvement were necessary.

426. ***Criterion 24.8*** – According to COC (§63^1), an undertaking may in addition to its address submit to the registrar the Estonian address of one person, which can be used for the delivery of the procedural documents of the undertaking. If the residence of at least half of the members of the management board of a private limited company, a public limited company or a branch is not in Estonia, in another Member State of the EEA or in the Swiss Confederation, the company is required to appoint the above-specified contact person. The authorities advise that regulations of COC (§63^1) identically apply to other forms of business entities, such as general partnerships, limited partnerships and commercial associations, as well as by non-profit associations and foundations, insofar as all these are "undertakings" defined by the law.

427. In any instance, this voluntary or, in case of companies with at least half of their management board located abroad, mandatory appointment of contact persons to receive incoming correspondence does not amount to a requirement that one or more natural persons resident in the country are authorized by the company, and accountable to competent authorities, for providing all basic information and available BO information, and giving further assistance to the authorities. According to COC (§631(2)) if the management board of a company or a body substituting therefor is located in a foreign state, the company must designate a contact person specified in COC (§63^1(1)). The authorities advise that, according to COC (§63^1(2)), in such case only a notary, advocate, law office, sworn auditor, audit firm, tax representative of a non-resident for the purposes of the Taxation Act or a provider of trust and company services specified in MLFPA (§8) may be designated a contact person. The address of the contact person shall be considered the address of the company in such case.

428. Other than the above-stated, there are no measures to ensure that companies cooperate with competent authorities to the fullest extent possible in determining the BO.

429. ***Criterion 24.9*** – MLTFPA (§47) requires OEs to retain the originals or copies of the documents obtained in the course of CDD, including those pertaining to identification and verification of identity of BO, no less than 5 years after the termination of the business relationship.

430. COC for general partnerships - §122 and for private limited companies – §219) and the NPAA (for non-profit associations - §54) provide for preservation of company documents after the liquidation/ removal of the legal entity from the register by way of depositing such documents with liquidators, persons maintaining archives or "another trustworthy person". Similar provisions on document retention for the other types of legal persons are provided as follows: for foundations – FA (§59); for commercial associations – GPCCA (94); for limited partnerships the provisions concerning general partnerships apply – COC (§125 (2)); for public limited companies – COC (§382). The authorities also advise that data retention by the CR and the NPAR is regulated in the Rules of Procedure of the Court Registry (§52 of), according to which: 1) for business entities – registry cards and business files are retained for an indefinite period of time; and 2) for non-business entities – registry cards are retained for an indefinite period of time, and public files are retained for 5 years after the removal of the entity from the register.

431. Overall, information made available to the assessment team does not enable a conclusion that the companies (or their administrators, liquidators or other persons involved in the dissolution of the company) are required to maintain the information and records referred to for at least 5 years after the date on which the company is dissolved or otherwise ceases to exist.

432. ***Criterion 24.10*** – With regard to accessibility of basic information, COC (§28) and NPAA (§77) define those entries in the CR and in the NPAR are public. Accordingly, competent authorities, including LEAs, may access such information as described in the analysis for c.24.3. According to MLTFPA (§78), the data of the BO are also made public in the e-Business Register and can be accessed free of charge by OEs, government agencies and courts. The authorities advise that, by a Government regulation (No. 369 from 04 December 2001) government agencies are required to use the central database of the court registry to ensure that at all times accurate and up-to-date information is used by all competent authorities. Such information comprises annual reports, articles of association and other documents submitted to the registry department of a court pursuant to law.

433. ***Criterion 24.11*** – The authorities advise that, since 2002, only shares registered with the ECRS are permitted in Estonia, and that every share registered in Estonia is entered into the register on a mandatory basis, including all shares of public limited companies (since 2003), all units of pension funds (since 2002) and all publicly traded bonds and investment fund units.

434. As to **private limited companies**, COC (§144) requires that names, personal identification codes or registry codes and addresses of shareholders, and the nominal value of the share of each shareholder are submitted to the CR for the registration of the company. According to COC (§149), a shareholder may freely transfer shares to a third person. The transaction constituting the obligation to transfer shares must be notarised, and the notary shall send a notice concerning the transfer of the shares to the registrar of the CR within two days after authentication of the contract.

435. According to COC (§228), shares of **public limited companies** shall be registered by way of entering them into the share register of the ECRS. COC (§233) defines that this share register should set out the name, address and personal identification code or registry code of the shareholders. COC (§229) establishes that registered shares may be freely transferred. At that, the transferee has the right – but is not obliged – to demand being entered as a shareholder in the share register. Whereas the shares of a public limited company shall be deemed to be transferred as of entry of the transferee in the ECRS, in circumstances where such shares are transferred to a third person without entering the transferee – who may act as the informal BO/ shareholder of the transferred shares – in the ECRS, they can be circulated as bearer shares for an indefinite period of time and with unlimited number of transfers, until any one of the transferees exercises the right of being entered in the share register.

436. ***Criterion 24.12*** – The COC, the NPAA and the FA do not distinguish between different types of directors; these acts do not recognise or provide for the formal status of a nominee director. All persons acting as directors have the same rights and duties under the mentioned acts. Likewise, the legislation does not recognise the formal status of a nominee shareholder, while the situations whereby someone might be the factual shareholder behind the person acting as the formal nominee shareholder are covered by the definition of BO in MLTFPA (§9) as the *"natural person who, via ownership… has final dominant influence over a natural or legal person"*. This means that potential instances of persons acting in the capacity of formal nominee shareholders would be identified by the AML/CFT system within the framework of CDD measures aimed at, *inter alia*, identification and verification of identity of BO.

437. ***Criterion 24.13*** – According to COC (§71), the registrar may, pursuant to the procedure provided by CCP and with or without first issuing the ruling of warning prescribed by it, impose a fine of no less than EUR 200 for the failure of an undertaking and any other person required to submit information to the register. CCP (Chapter 58) regulates matters concerning registers maintained by Tartu District Court, including the registers of commercial companies, non-profit associations and foundations.

438. According to CCP (§601), if the court has certified information on the entry of incorrect data in a register, or on failure to submit data subject to entry in the register pursuant to law, the court makes an order whereby the persons obligated to submit the data are ordered to submit correct data or file an objection against the order, and are cautioned that failure to comply may result in the imposition of a fine. CCP (§46) defines that such fine may be imposed to the extent of up to EUR 3 200. In determining the amount of a fine, the court takes the financial situation of the person and other circumstances into consideration.

439. According to Penal Code (§281) submission of incorrect information to the registrar of the CR, registrar of the non-profit associations and foundations register, the central securities depository, a notary or an enforcement agent is punishable by a pecuniary punishment or up to two years' imprisonment. The same act, if committed by a legal person, is punishable by a pecuniary punishment.

440. Moreover, MLTFPA (§84 and §85) define that the penalty for the breach by an obliged entity or its management board member or an employee of the duty to identify and verify the identity of customers and BOs is a fine of up to 300 fine units or detention, while the penalty for the same act committed by a legal person is a fine of up to EUR 400 000. On the background of this significant amount of the fine stipulated for AML/CFT non-compliance of a legal person, the fine determined under COC (§71) and its maximum amount established under CCP (§601) do not seem proportionate and dissuasive.

441. ***Criterion 24.14*** – As regards basic and BO information available through the Estonian registers, i.e., the CR, the NPAR and the BOID, these are public sources, and relevant information may be obtained by any foreign competent authority directly or through the European Business Register[269]. The latter is an additional service of the e-Business Register mediating official information about European companies[270].

442. Concerning basic and BO information maintained by companies and OEs in terms of its availability for international cooperation, see the analysis for Recommendations 37-40 on the methods and tools, including investigative powers, used by competent authorities in accordance with Estonian law to exchange shareholder information and obtain BO information on behalf of foreign counterparts. Deficiencies in R.3740 have bearing on the rating here.

443. ***Criterion 24.15*** – The authorities advise that there are no centralised mechanisms – either at national or at agency levels – for monitoring the quality of assistance received from counterparts in other countries in response to requests for basic and BO information or requests for assistance in locating BOs residing abroad.

444. The EFIU considers that the information received from international counterparties is usually correct and accurate. In 2020 it has published the Annual Overview of International Cooperation[271]. The EFIU assesses the quality of received foreign requests, as well as the quality and timeliness of the responses received from foreign counterparties. Regarding basic and BO information, the EFIU relies both on different open-source solutions and those offered by different vendors, and indeed on information provided by foreign counterparts on specific subjects. If various sources provide different results, further scrutiny is carried out.

445. The EFSA assesses the quality of information requests on a case-by-case basis. The expectation is always to receive a response to assistance requests and, in case there is no response, a "kind reminder" letter is sent to the relevant authority. Where the response does not reflect on all aspects of the request, further clarifications are sought via e-mail or, if necessary, additional formal communication. According to the FSA Act (§47(21)), if a request of the Supervision Authority for the receipt of information, commencement of supervision proceedings or performance of any other such action, as well as for the presence of the employees of the

[269] Also accessible through the European Business Register Network (https://ebra.be/european-business-register-network/)
[270] Additional information on the countries participating in the EBR initiative is available at https://www.rik.ee/en/european-business-register/list-states
[271] https://fiu.ee/en/media/138/download

Supervision Authority in proceedings organised by the financial supervision authority of the other Contracting State is not performed within a reasonable period of time or if the request is rejected, the Supervision Authority may notify of such rejection or non-performance within a reasonable period of time the relevant European supervisory authority.

446. Other authorities, e.g., the ISS, advise of monitoring the quality of assistance on a general basis only. The PBGB assesses the quality of information received in response to a request for mutual legal assistance on case-by-case basis, and no central control is applied (due to lack of centralised data on the quality of responses). In case of shortcomings in a request for MLA, feedback is sent to the Prosecutor's Office and, if necessary, the partner country is asked to supplement the data. In the case of operational information, the requesting authority assesses the quality of responses and, if necessary, asks for the response to be supplemented or makes a new request with reference to the shortcomings in the previous response. The ETCB analyses the quality of the received information on case-by-case basis. Information on BOs received from foreign counterparts is assessed in the course of the proceedings and, as a general rule, the information received is correct (compared to the information in CRs).

Weighting and Conclusion

447. Among requirements that are partly met, the following are considered to have a heavier weight in determining the rating for this Recommendation: available analyses do not appear to provide a reliable assessment of the ML/TF risks associated with all types of legal persons created in the country (c.24.2); the regulations in place do not provide for a number of elements of the FATF requirements for maintaining basic information (c.23.4); there are insufficient mechanisms to ensure that basic information is accurate and updated on a timely basis (c.24.5); there are insufficient measures to ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner (c.24.8); and information made available to the assessment team does not enable a conclusion that the companies are required to maintain the information and records referred to for at least 5 years (c.24.9). **R.24 is rated PC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

448. In the 4th round MER of 2014, Estonia was rated non-applicable with former R.34. The assessment concluded that legal arrangements do not exist as an entity in the legal system of Estonia. With respect to foreign legal arrangements, the authorities clarified that a legal arrangement is not considered to be a legal person, i.e., to have legal capacity in its own right to be in a contractual relationship with an obliged entity.

449. ***Criterion 25.1*** – Trusts or other similar legal arrangements, which would fall within the FATF Glossary definition, do not have legal capacity in Estonia; therefore, it is not possible to create or establish an express or any other trust under Estonian law. Accordingly, c.25.1(a) and c.25.1(b) are non-applicable.

450. As to professional trustees[272] considered under c.25.1(c), MLTFPA (§7[1]) defines the notion of a trustee as the person who administers the trust property formed by the settlor *"in the trustee's own name but in the interests of beneficiaries or for another defined purpose"*. With regard to this, MLTFPA (§2(6)) establishes that Chapter 9 of the law – and specifically MLTFPA (§76-77) defining requirements for private legal persons to gather and keep with the CR BO information –

[272] E.g. lawyers or trust companies paid to act as a trustee in the course of their business

also apply to trustees. However, this requirement is partially enforceable (see the analysis for c.25.7), therefore trustees are subject to the obligations set out in c.25.1 to a limited extent.

451. Given the MLTFPA definition of BO of a trust (which covers all subjects specified under c.25.1(a))[273], it can be concluded that MLTFPA sets out the requirement for trustees to obtain information specified under the c.25.1(a). However, there is no effective requirement for trustees to maintain the information specified under the c.25.1(a), as MLTFPA (§76(1^2)) requires trustees to "gather and keep with the Commercial Registry" data of BO, i.e., technically there is no requirement for trustees to hold the information themselves. Moreover, there is no requirement for trustees to obtain and maintain information specified under the c.25.1(b) (i.e., basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors) for at least 5 years after their involvement with the trust ceases.

452. ***Criterion 25.2*** – This criterion is not applicable to Estonia as regards trusts governed under domestic law, which are non-existent, and it is not appropriately met as regards professional trustees acting for a trust or other legal arrangements under foreign law, due to the reasons articulated under the analysis for c.25.1. At the same time, all obliged entities have to maintain accurate and up-to-date information about settlor or protector, trustee, or beneficiaries of a trust (MLTFPA §9, §20 and §21).

453. ***Criterion 25.3*** – MLTFPA (§46) requires OEs to register, upon making transactions with a trust or trustee, the fact that the person has such status, through an extract of the registry card or a certificate of the registrar of the register, where the legal arrangement has been registered. The authorities advise that transactions referenced in this provision include not only occasional transactions, but also *"separate transactions in the course of economic, professional or official activities"* that are part of the business relationship defined under MLTFPA Section 3(4). Overall, the mentioned provision does not establish an obligation for trustees to disclose their status to FIs and DNFBPs when forming a business relationship or carrying out an occasional transaction and, as such, does not amount to a sufficient measure ensuring compliance with the requirement under this criterion.

454. ***Criterion 25.4*** – There are no provisions in law or other enforceable means – and no appropriate obligations to have the effect of – requiring trustees to provide competent authorities with any information relating to the trust other than BO information gathered and reported to the BOID. This means that the requirements in this criterion would be met to the extent allowed by the deficiencies identified under the analysis for c.25.1 and that, whereas there are no legislative or otherwise enforceable provisions in the Estonian law to prevent trustees from providing further information to the competent authorities, trustees would be governed under the general regulation (of the foreign law) to maintain client secrecy, thus effectively preventing them from providing such further information to the competent authorities.

455. As to providing FIs and DNFBPs, upon request, with information on the BO and the assets of the trust to be held or managed under the terms of the business relationship, MLTFPA (§28) establishes the obligation of FIs to gather sufficient information on the beneficiaries of a trust or

[273] According to MLTFPA §9(6), beneficial owner of a trust or a legal arrangement is defined as the settlor of the trust or the establisher of the arrangement; the trustee; the person ensuring and controlling the preservation of property, where such person has been appointed; the beneficiary, or where the beneficiary or beneficiaries are yet to be determined, the class of persons in whose main interest such triste or arrangement has been set up or operates; any other person who in any way exercises ultimate control over the property of the trust or arrangement.

a legal arrangement. Such regulation does not create an obligation for the trustees (or to put it otherwise, does not overcome the practical barrier, as described in the paragraph above, preventing them) to provide, upon request, relevant information to credit and financial institutions, and it does not cover the element of providing information on the assets of the trust to be held or managed under the terms of the business relationship.

456. ***Criterion 25.5*** – BO information reported by the trustees to the CR is accessible for the competent authorities as set out in the analysis for c.24.10. As to other information held by trustees (e.g., the residence of the trustee, or the information to be obtained under c. 25.1(b)) or by FIs and DNFBPs (e.g. any assets held or managed by them in relation to any trustees, with which they have a business relationship, or for which they undertake an occasional transaction), the assessed country advises that LEAs have all powers necessary to be able to obtain timely access to information held by trustees, other DNFBPs and FIs (see c.31.1). The general standards on access by competent authorities to information held by regulated entities apply to information about assets held or managed by FIs and DNFBPs, (cf. criteria 27.3, 28.4 and 29.3).

457. ***Criterion 25.6*** – As regards basic and BO information available through the Estonian registers, i.e. the CR, the NPAR and the BOID, these are public sources, and relevant information on trusts and other legal arrangements, if any, may be obtained by any foreign competent authority directly or through the European Business Register[274]. The latter is an additional service of the e-Business Register mediating official information about European companies[275].

458. Concerning domestically available information on trusts and other legal arrangements maintained by trustees and OEs in terms of its availability for international cooperation, see the analysis for Recommendations 37-40 on the methods and tools, including investigative powers, used by competent authorities in accordance with Estonian law to exchange such information and obtain beneficial ownership information on behalf of foreign counterparts. Deficiencies in R.3740 have bearing on the rating here.

459. ***Criterion 25.7*** – Under the current regulations in Estonian law, trustees are subject to the obligations set out in c.25.1-c.25.2 to a limited extent. Moreover, the liability for the failure to comply with these obligations is partially enforceable. Particularly, MLTFPA (§95) establishes a penalty of 300 fine units[276] for the failure of a trustee *"to submit the details of the beneficial owner or for failure to report on a change of the details or for knowingly submitting false information, where it has caused a situation where the obliged entity cannot apply the due diligence measure"*. Accordingly, enforceability of the requirement for trustees to gather and report trust-related BO information to the CR is provided to a limited extent, insofar as it applies to cases where non-provision of information to the obliged entity has resulted in latter's inability to conduct CDD but does not apply to cases where the trustee has failed to report BO information to the BOID.

460. ***Criterion 25.8*** – As set out in the analysis for c.25.7, enforceability of the requirement for trustees to gather and report trust-related BO information to the CR is provided to a limited extent. No sanctions are available for the failure of trustees to otherwise grant to competent authorities' timely access to information held by them. Failure to ensure that information held with the OE is made available to competent authorities swiftly upon request is punished by

[274] Also accessible through the European Business Register Network (https://ebra.be/european-business-register-network/)

[275] Additional information on the countries participating in the EBR initiative is available at https://www.rik.ee/en/european-business-register/list-states

[276] According to Penal Code §47(1), a fine unit is the base amount of a fine and is equal to EUR 4.

imposition of coercive measures in the form of a non-compliance levy, i.e., a penalty payment (MLTFPA, §47(4), §65; FSAA, §18(2)4), §55(1)).

Weighting and Conclusion

461. Among requirements that are partly met, the following are considered to have a heavier weight in determining the rating for this Recommendation: there is no effective requirement for trustees to maintain the information specified under c.25.1(a), as well as to obtain and maintain information specified under c.25.1(b) (c.25.1(c)); there are no sufficient measures in place to ensure that trustees disclose their status to financial institutions and DNFBPs (c.25.3); the arrangements in place would effectively prevent trustees from providing relevant information to competent authorities, financial institutions and DNFBPs (c.25.4); liability for the failure of trustees to comply with relevant obligations is partially enforceable (c.25.7); and no sanctions are available for the failure of trustees to otherwise grant to competent authorities' timely access to information held by them (c.25.8). **R.25 is rated PC.**

Recommendation 26 – Regulation and supervision of financial institutions

462. In the 4th round MER of 2014, Estonia was rated LC on R.23. The report noted several issues in relation to effectiveness, including the insufficient ongoing supervision and monitoring of several FIs (investment firms, life insurance companies and payment service providers) and the low capacity and ineffective supervisory activity by the FIU. Effectiveness issues are now covered under IO.3.

463. The introduction to R.10 lists the activities to which the MLTFPA does not apply, and which are not subject to regulation and supervision for AML/CFT purposes. Nevertheless, the companies managing mandatory pension funds and life insurance companies providing services related to mandatory funded pension insurance contracts are licenced and supervised for prudential purposes pursuant to IFA, §§3(2)(4), 455 and IAA, §§15, 223.

464. ***Criterion 26.1*** – The EFSA and the EFIU are designated to supervise the covered FIs' compliance with the AML/CFT requirements. (MLTFPA, §64(1)(2)). The EFSA supervises the vast majority of the FIs – banks, PSPs, EMIs, investment firms, fund managers, consumer credit providers and insurance companies. Companies managing a mandatory pension fund and life insurance companies providing services related to mandatory funded pension insurance contracts within the meaning of Funded Pensions Act are excluded from the scope of AML/CFT supervision. There is no formal assessment (in the NRA or other documents) that would justify these exemptions, although the authorities provided arguments concerning the very low ML/TF risk due to the funding nature – preliminary funding from the employment salary through the Tax and Customs and partly directly from the government through taxation of said salary, and the possibility to withdraw the funds after retirement.

465. The EFIU is responsible for the supervision of the currency exchange offices, credit providers who are exempted from the CCIA, such as those who provide services for legal persons, financial leasing, guarantees and commitments service providers, small fund managers without an activity licence obtained from the EFSA, money broking service providers[277] and savings and loan associations.

466. The supervisory responsibilities include the oversight of the branches of foreign credit

[277] Providing services based on a brokerage contract (Art. 658 Law of Obligations Act).

institutions and foreign financial service providers registered in the Estonian CR (MLTFPA, §6(1)2) and (2)12)). This excludes the provision of cross-border services by the EEA FIs under the EU principle of the freedom to provide services[278], which requires only a prior notification of such operations.

467. Supervision of TFS obligations is carried out based on the ISA provisions. Until 2021, the EFIU was the only authority exercising the supervision of all FIs. Due to the 2020 amendments of the ISA, the competence is shared with the EFSA, the last being responsible for the credit institutions and FIs under its supervision (ISA, §30(1)(1^1)).

468. ***Criterion 26.2 –*** All FIs, including Core Principles FIs, must be licenced or authorised by the EFSA or EFIU before carrying out activities in Estonia (MLTFPA, §70(1)(2)). The FIs which hold or are required to apply for the EFSA's authorisation, are exempted from the obligation to apply for an authorisation by the EFIU (MLTFPA, §70(1)(2)). Requirement for licensing of Core Principles FIs is also outlined under the appropriate sector-relevant acts (CIA, §13; PIEIA, §14; SMA, §48; IFA, §313 and §441; CCIA, §10; IAA, §15;). Small fund managers who did not apply for an activity licence pursuant to §441 of the IFA, must registered by the EFSA (IFA, §306(3)) and obtain an authorisation from the EFIU (MLTFPA, §70(1)). Currency exchange offices are required to be licenced by the EFIU based on §70(1) of the MLTFPA.

469. Conducting any economic activity without an activity licence constitutes a criminal offence (§372 of the CC).

470. In order to be licenced, the registered office and head office of banks must be in Estonia, thus the establishment and operation of shell banks is not allowed in Estonia (CIA, §§13(2), 15(1)).

471. ***Criterion 26.3*** – The MLTFPA and sector specific laws set out varying market entry control measures to prevent criminals or their associates from holding, or being the BO of, a significant controlling or holding a management function in an FI.

FIs under the EFSA's supervision

472. In order to ensure that no criminals (or their associates) hold, or are the BO of, a significant controlling interest in a FI, the EFSA carries out fit and proper assessment under the sectoral laws. In case of credit institutions, a qualifying holding[279] may be acquired, held or increased and the control may be achieved, held and increased only by a person who has an "impeccable business reputation" and with respect to whom there is no justified suspicion that the acquisition, possession or increase of the holding or the control is connected to ML or TF or any attempts thereof, or increases such risks. In the course of the acquisition, the person shall also comply with the principles of "sound and prudent" management of a credit institution (CIA, §29^{1}1)5), §31(3)). These requirements have a broad scope and include, as highlighted by § 48(2) of the CIA, the Guidelines issues by the EFSA (mentioned below) and confirmed by the practice, checking whether the person has been convicted of an offence, accused or suspected of an offence, or otherwise involved in an offence, or the person has committed an unlawful, fraudulent or abuse of confidence act or ML or TF, or has been involved in that act or in its investigation or surveillance proceedings. Similar requirements are in place for creditors and credit intermediaries (CCIA,

[278] Which has to be exercised on a temporary and occasional basis.

[279] A "qualifying holding" means a direct or indirect holding in an undertaking which represents 10 % or more of the capital or of the voting rights or which makes it possible to exercise a significant influence over the management of that undertaking (CIA, § 29 (5) referring to art. 4 (36) of the EU Regulation No 575/2013).

§29(1)1), 6), §34(1)1)), PSPs and EMIs (PIEIA, §38 1), 5) and §43(1)1)), fund management companies (IFA, §322 1), 5), §327 (1)1)), investment firms (SMA, §72 1), 5), §76(1) 1)), and insurance companies (IAA, §117(1)1), 5), §120(3)1)).

473. In addition, the EFSA also has powers to "reverse" its decision that allows the acquiring of a qualifying holding or limit the voting rights of the existing owners of a qualifying holding, if it determines that the persons are no longer in compliance with the fit and proper requirements (CIA, §31(3)(5)(6); CCIA, §34(3); PIEIA, §43(3)(4); IFA, §327(3)(4); SMA, §76(3)(4); IAA, §120 (5)(6)).

474. The members of the supervisory board and management board of FIs also have to meet fit and proper requirements pursuant to sectoral laws and on an ongoing basis. The key requirements of the fit and proper assessment are the "impeccable business reputation" and the professional qualifications and skills (including the necessary expertise, experience and education). The person is also considered unfit if: i) their earlier activities have caused the bankruptcy, compulsory liquidation or revocation of the activity licence of a company; ii) their right to engage in economic activity has been taken away pursuant to law; iii) their earlier activities as a manager proved to be unsuitable and inadequate (CIA, §48(2)(3)). Similar fit and proper requirements for managers are in place for creditors and credit intermediaries (CCIA, §39(1)1), (2)1), 3), 4), (3)), PSPs and EMIs (PIEIA, §47(1) and (4)1)-3), 5)), fund management companies (IFA, §310(3)(4)1)4)), investment firms (SMA, §79(1)(4)1)-3)), and insurance companies (IAA, §106(1)(2)1), 4)-5).

475. In the case of credit institutions, the "impeccable business reputation" requires checking whether the person has been convicted of an offence, accused or suspected of an offence, or otherwise involved in an offence, or has committed an unlawful, fraudulent or abuse of confidence act or ML or TF, or has been involved in that act or in its investigation or surveillance proceedings (CIA, §48(2)). Apart from the CIA, the sectoral laws make reference to a non-exhaustive list of "unfit" qualities, which do not comply with the "impeccable business reputation" requirement, and include *inter alia*: i) a conviction for a first-degree crime (CCIA, §39(2)2); IFA, §310(4)2); IAA, §106(2)2)); ii) a conviction for an economic offence, official misconduct, offence against property or offence against public trust or the financing or supporting of an act of terrorism (CCIA, §39(2)6); PIEIA, §47(4)4); IFA, §310(4)3); SMA, §79(4)4), IAA, §106(2)3)). In practice, irrespective of the non-exhaustive specific requirements, the EFSA has large discretionary powers for determining whether a person has impeccable reputation, which include their criminal records, involvement in the criminal proceedings or their association with criminals.

476. The EFSA also has powers to order the recall of an unsuitable member of the board (CIA, §50(1), §104(1)9), 10); CCIA, §42(1), §91(1)6); PIEIA, §49, §101(1)5); IFA, §312, §458(1)5); SMA, §81(1), §235 6), 7); IAA, §108 (1), §228 (2)12)).

477. In relation to the Estonian significant credit institutions[280] which are under direct supervision of the ECB within the framework of the Single Supervisory Mechanism (SSM), the ECB is the competent authority for taking decisions on qualifying holding procedures and appointment of all members of the management bodies. In this respect, the EFSA follows the internal policy and public guidelines issued by the ECB.

[280] Currently, there are 3 credit institutions under the ECB's direct supervision, see: https://www.fi.ee/en/financial-supervision/international-cooperation/single-supervisory-mechanism-ssm#:~:text=The%20SSM%20is%20intended%20to,SEB%20Pank%20and%20Luminor%20Bank

478. The EFSA has published the Guidelines for conducting fit and proper assessment of 15.10.2018[281], which explains to the market participants the process and the main expectations, and also covers the requirements for the persons holding significant or controlling interests. It has implemented the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/12/2017), via the EFSA decision of 30.06.2018 (in force until 31.12.2021)[282]: and the Joint EIOPA, EBA and ESMA Guidelines on prudential assessment of acquisitions and increases of qualifying holdings in the financial sector (KC/G L/2016/01), via its decision of 24.07.2017 (in force since 01.10.2017)[283]. For internal purposes, the EFSA has issued a Handbook on the fit and proper process, which defines the minimum requirements for carrying out the fit and proper assessment.

FIs under the EFIU's supervision

479. The fit and proper assessment carried out by the EFIU requires that the applicant, including the owner, BO and the members of the management body: i) does not have any unspent conviction for a criminal offence against the authority of the state, offence related to money laundering or other intentionally committed criminal offence; ii) has a proper business reputation (MLTFPA, §72(1)1) and 1[1]). In the case of the members of the management body, the applicant must submit documents that prove their *trustworthiness* and the proper business reputation (MLTFPA, §70(3)10)). A person is deemed not to possess a proper business reputation of the EFIU has ascertained facts that cast doubt on the presence of such reputation or confirm its absence. Similarly with the requirements established for the FIs under the EFSA supervision, the MLTFPA provides for a non-exhaustive list of "unfit" qualities, which do not comply with the "proper business reputation" requirement: i) a conviction for a first-degree crime; ii) a conviction for an economic offence, for an offence relating to public office, for an offence against property, against public trust, a terrorist or TF offence, the person is subject to international sanctions; iii) person's earlier actions/ omissions let to the bankruptcy or the revocation of the authorisation of an undertaking or of another entity under financial supervision; iv) the person is subject to disqualification from certain professional activities; v) the person has filed previously false information with the EFIU, or failed to file material information (MLTFPA, §72(2)). The requirement of *proper business reputation* is interpreted in a broad manner and covers the association with criminals. This is also confirmed by the explanatory memorandum of the draft MLTFPA, which details that the assessment of the reputation shall take into account the person's past conduct (acts, media coverage, punishment, involvement in legal proceedings, participation in business, society's assessment of the person) and that due the enduring nature of the reputation, it does not depend solely on technical or legal nuances and it cannot be erased or considered obsolete in certain respects.

480. Similarly to the EFSA, the EFIU can also revoke an authorisation (MLTFPA, §75 4)).

481. ***Criterion 26.4*** – (a) Estonia's Financial Sector Assessment Program (FSAP) report was conducted in 2000[284] and the assessment of the country's compliance with the IOSCO Principles was carried out prior to becoming a signatory to the IOSCO MMOU in 2011.[285] Given the significant

[281] https://www.fi.ee/et/juhendid/pangandus-ja-krediit/sobivusmenetluse-labiviimise-juhend
[282] https://www.fi.ee/et/juhendid/investeerimine/suunised-juhtorgani-liikmete-ja-votmeisikute-sobivuse-hindamise-kohta
[283] https://www.fi.ee/et/juhendid/banking-and-credit/uhissuunised-finantssektoriga-seotud-olulise-osaluse-omandamise-ja-suurendamise
[284] https://www.imf.org/external/np/rosc/est/insurance.htm
[285] https://www.iosco.org/news/pdf/IOSCONEWS204.pdf

time since the last external evaluations, their conclusions are no longer considered to be relevant. The regulation and supervision of core principles institutions are considered by the authorities to be in line with the core principles which are relevant to AML/CFT, due to their implementation into the national legislation. The relevant domestic acts which are considered to implement the BCBS Principles are: the CIA, which establishes the requirements for banks and their supervision; the FSAA which regulates the role, rights, powers and resources of the supervisor, including the application of consolidated group supervision; the MLTFPA – the specific requirements for AML/CFT related corporate governance, risk management and CDD rules. The IOSCO Principles and responsibilities[286] applicable for investment and fund management service providers and their supervision are considered by the authorities to be implemented into the national legislation by the IFA, SMA, FSAA and MLTFPA. Nevertheless, there is no a self-assessment report that would confirm these conclusions. The authorities also made reference to the 2019 IMF report on Estonia's progress in strengthening AML/CFT supervision[287], which acknowledged a series of enhancements to the AML/CFT framework and recommended the authorities to make further efforts for increasing the number of on-site AML/CFT inspections, raising the penalties for AML/CFT violations, and consolidating the supervision at the regional level. Although relevant in some respects, the scope of the 2019 IMF assessment is considerably limited compared to that of the Core Principles which are relevant to AML/CFT.

482. The assessment of Estonia against the Insurance Core Principles (ICP) of the IAIS was carried out in 2000 as part of the Financial Sector Assessment Programme (FSAP) and in 2011 when Estonia applied for OECD Membership. Estonia was found to be compliant with the ICP including appropriately imposing AML/CFT controls on insurers. In August 2021, the IAIS conducted a Peer Review Process on Supervisory Review and Reporting (ICP 9) and Preventive Measures, Corrective Measures and Sanctions (ICP 10), which found (draft report in May 2022) that the standard of ICP9 is observed and of ICP10 is largely observed.

483. (b) The same regulatory and supervisory principles apply to both, core principles and non-core principles covered FIs, which require a risk-based approach to supervision.

484. ***Criterion 26.5*** – The EFSA is required to perform its tasks in a risk-based manner. The frequency and scale of on-site and off-site AML/CFT inspections must be based on the: (a) ML/TF risks, policies, internal control and procedures associated with the entity/ group; and (b) the ML/TF risks present in Estonia (EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §5.1). The frequency and the scale of the supervisory activity must be based on the results of the Sectoral Risk Assessment, Risk Dashboard and the Risk-Based Approach Model (EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §5.8). The supervisory circle foresees actions: (i) every year for high and very high-risk entities; (ii) every three years for medium-risk entities; (iii) every five years for low-risk entities; and (iv) only off-site supervision for very low-risk entities (EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §5.5).

485. The supervisory approach of the EFIU outlined by the Code of Conduct for the Supervision Activities requires the application of a risk-based supervision (§1.5). It shall minimally take into consideration: the results of the NRA; the analysis carried out by the EFIU; the quantity and quality of the received notifications (STRs and other type of reports); the previously known threats and vulnerabilities. In 2021, the EFIU developed a Risk matrix tool, which is data-driven,

[286] Principles 24, 28, 29 and 32; Responsibilities A, B, C and D
[287] https://www.imf.org/en/Publications/CR/Issues/2020/01/21/Republic-of-Estonia-2019-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-48963

based on the combined analysis of the licensing data from the Register of Economic Activity, BR's business field data and the EFIU database data (numerical indicators of ML/TF suspicion: STRs, CTRs, TFRs, law enforcement and international queries, EFIU analysis dossiers) regarding potential higher-risk market participants. The tool became the main document for risk assessment and selecting entities for supervisory activities. Although not formalised under the Code of Conduct, the authorities advised that the cycle of inspections is impacted by the risk profile of the sector and of the individual business: (i) high and medium high-risk entities – annually; (ii) medium risk entities – 3-4 years; (iii) medium low entities – 5 years; and (iv) low risk entities are supervised with off-site inspections. The cycle of inspections can be subject to deviation in certain circumstances, such as, poor AML/CFT knowledge of the sector, new typologies, and emerging risks in the supervised sectors.

486. It is not clear how the RBA models of the EFSA and the EFIU take into account the degree of discretion allowed to the covered FIs under the risk-based approach.

487. ***Criterion 26.6*** – The EFSA is required to review periodically the assessment of the ML/TF risk profile of the FIs under its supervision: (i) each year for credit institutions, life insurance companies, securities firms, PSPs, EMIs and the branches of these institutions; (ii) every two years for fund managers and consumer credit provides (due to the residual lower risk assigned to these sectors), as well as when there are indications of new or emerging risks (EFSA AML Rules of Procedure, Chapter 6: Risk-based approach model, §1.12, §3.3). The Code of conduct for the supervision activities of the EFIU does not provide for such periodical reviews. Nevertheless, 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.

Weighting and Conclusion

The following shortcomings have been identified, which are considered to be minor: the authorities have not fully demonstrated the regulation and supervision of core principle institutions are in line with the relevant core principles; it is not clear how the RBA models of the EFSA and the EFIU take into account the degree of discretion allowed to the covered FIs under the risk-based approach; the EFIU is not required formally to review periodically and, in case of major events or developments, the assessment of the ML/TF risk profile of the of the supervised sectors; the conclusions to R.10 regarding the scope of application of the MLTFPA are relevant here and have an impact on the regulatory and supervisory regime of the FIs. **R.26 is rated LC.**

Recommendation 27 – Powers of supervisors

488. In the 4th round MER of 2014, Estonia was rated LC on R.29. The report noted the lack of adequate sanctioning powers against directors and senior management for breaches by a financial institution.

489. The introduction to R.10 lists the activities to which the MLTFPA does apply, and therefore are not subject to regulation or supervision.

490. ***Criterion 27.1*** – Designated supervisors, the EFSA and the EFIU, have powers to supervise the FIs and take appropriate measures to ensure compliance with AML/CFT requirements (MLTFPA, §54(1)4), §64(1)(2); FSAA, §6(7); SFIU, §7(4)). The EFSA is the supervisor of most FIs (see c.26.1) and its powers to exercise supervision over the specific sectors are also outlined in the relevant sectoral acts (CIA, Chapter 9 *Supervision*; CCIA, Chapter 13 *Supervision*; PIEIA, Chapter 12 *Supervision*; IFA, Chapter 30 *Supervision*; IFA, Chapter 30 *Supervision*; IAA, Chapter 12

Supervision; SMA, Chapter 24 *Supervision*). The powers of both designated authorities to exercise supervision over FIs include the power to conduct on-site and off-site inspections, to obtain documents and data without limitations, to receive oral and written explanations from an OE, members of its management body and employees (MLTFPA, §66).

491. The EFSA and the EFIU are also responsible for the supervision of FIs' compliance with TFS obligations (ISA, §30(1)(1^1)). The authorities are obliged to cooperate and exchange information, especially in the case of an identified or suspected violation of the TFS obligations, and the EFSA is required to promptly inform the EFIU of such cases (ISA, §33).

492. ***Criterion 27.2*** – Both designated supervisors have powers to conduct on-site and off-site inspections of FIs, or a combination of both methods. The inspections can be targeted, thematic or full scope. This includes the right to inspect the seat or the place of business of the OE, to enter (in the presence of a representative of the inspected person) any building or room, as well as to require inspection, without limitations, of documents and data, receive oral and written explanations, and monitor any work processes (MLTFPA, §66; AML Rules of procedure of the EFSA, §2.6; Code of conduct for the supervision activities of the EFIU, §2.2). The EFSA also has the right to initiate an ad-hoc on-site inspection (without prior notification) when there is a suspicion that the prior notice might, *inter alia,* trigger withholding and/or deletion of information by the supervised entity and/or when the purpose of the on-site inspection cannot be achieved otherwise[288] (AML Rules of procedure of the EFSA, §7.8).

493. The same powers are available to conduct inspections to supervise compliance with TFS obligations (SFIU, §6(7), in conjunction with §1.1 and §2.2 of the Code of conduct for the supervision activities of the EFIU; FSAA, §6 (7), 22^1 3), in conjunction with §2.4 and §2.6 of the AML Rules of procedure of the EFSA).

494. ***Criterion 27.3*** – Supervisors are empowered to compel FIs to provide information without the need for a court order. The powers include the right to require and examine, without limitation, any documents and data, make extracts, transcripts and copies of those documents and data, as well as to receive oral and written explanations from an OE, members of its management body and employees (MLTFPA, §66). The powers also comprise the right to request information from third parties, including other state authorities and local authority agencies (MLTFPA, §58(1); FSAA, 22^1(1)1)). The EFSA also has the power to request the appearance of the OEs under its supervision and of third persons at its offices, in connection with provision of information relevant to financial supervision (FSAA, 22^1(1)2)). Non-compliance may result in a "non-compliance levy". In case of a natural person - up to EUR 5 000, which can be increased up to EUR 50 000 on any subsequent occasion. In case of legal persons – up to EUR 32 000 on the first and up to EUR 100 000 on any subsequent occasion (but not higher than EUR 5 mil or 10% of the total annual turnover (MLTFPA, §65(2)).

495. ***Criterion 27.4*** – The designated supervisors for the covered FIs are authorised to impose a variety of sanctions. The shortcomings identified under R.35 apply (see R.35).

Weighting and Conclusion

496. Shortcomings underlined under the conclusion to R. 10 with regard to the scope of application of the MLTFPA and to R.35 regarding the effectiveness, proportionality and dissuasiveness of the available sanctions are also relevant here. **R.27 is rated LC**.

[288] Since 2014, 2 such unannounced inspections were carried out by the EFSA.

Recommendation 28 – Regulation and supervision of DNFBPs

497. In the 4th round MER of 2014, Estonia was rated PC on R.24. The report noted several issues in relation to effectiveness, including insufficient supervisory resources at the EFIU, low level of on-site visits for certain DNFBPs under EFIU supervision and limited range of sanctions applied by the EFIU (only misdemeanour proceedings), insufficient supervision undertaken by the BA and CN and lack of sanctions imposed by the SRBs. Effectiveness issues are now covered under IO.3.

498. R.22 lists the activities to which the MLTFPA does not apply and, therefore, are not subject to AML/CFT regulation and supervision.

499. ***Criterion 28.1*** – Casinos in Estonia are subject to AML/CFT regulation and supervision.

500. (a) Gambling operators are required to have an activity licence which is issued by the ETCB, pursuant to the conditions established by Subchapter 2 of the Gambling Act (GA, §9(1), Subchapter 2). The ETCB is also entitled to revoke an activity licence (GA, §20). Operating without a licence is a criminal offence, which is punishable by a fine or up to three years of imprisonment (PC, §372).

501. (b) Measures are in place to prevent criminals and their associates from owning, being a BO, controlling, managing or operating a casino. The fit and proper criteria for the shareholders with a qualifying holding, the BO and the management body require the lack of a criminal record, trustworthiness and a good reputation (GA, §9(1), §11(2), §17(2)). A qualifying holding in a gambling operator is considered any direct or indirect holding in the share capital, which represents 10% or more of the share capital, of all rights related thereto or of the voting rights, or which makes it possible to exercise a significant influence over the management of the company (GA, §11(1)). An acquisition or increase of qualifying holding would be subject to the same fit and proper requirements (GA, §12(1)). The ETCB has the right to inspect the applicant in order to verify the compliance with the legal requirements (GA, §18). The licence may be revoked if the holder does not fulfil anymore the established fit and proper requirements, including when the holder of the activity licence has been involved in ML or repeatedly violated the AML/CFT procedure (GA, §20(1)(2)).

502. (c) The EFIU is the designated supervisor for the compliance with AML/CFT requirements by the gambling operators (except for organisers of commercial lotteries)[289] (MLTFPA, §64(1)).

503. ***Criterion 28.2*** – The EFIU is the designated supervisory authority for all covered DNFBPs, except for lawyers and notaries (MLTFPA, §64(1)). Notaries are supervised by the CN [290] and lawyers – by the BA (MLTFPA, §64(3)(4); NA, §44(2) 3^1), NRA, §75). The ISA designates the same authorities for the supervision of the covered DNFBPs regarding the compliance with the TFS obligations (ISA, §30(1)(4)-(5)).

504. The CN, as a self-regulatory body, is under the administrative supervision of the Ministry of Justice, including in the delegated area related to AML/CFT supervision. The powers of the MoJ include, *inter alia,* the right to give instructions, amend resolutions adopted by the CN and file protests with administrative courts against the legal acts/ measures taken by the bodies of the Chamber (NA, §5(2), §43(4)). The supervision of the BA is ensured by the MoJ and administrative

[289] Commercial lottery, as defined by the GA, §6, is not covered by the FATF standards.
[290] Under §75 of the Notarial Regulation Act, the MoJ has delegated the responsibility for the supervision pursuant to the MLTFPA to the CN.

court. The MoJ has the power to file a protest against a legal instrument or operation of a body of the Bar in the administrative court, contest the decisions of the Ethics Tribunal in administrative court, request any documents adopted by the bodies of the Bar, except those subject to attorney-client privilege. Likewise, any interest person may file a complaint against a legal instrument or an operation of a body of the Bar with the administrative court (BAA, §4(3)-(6)).

505. ***Criterion 28.3*** – Designated supervisors of the covered DNFBPs are required to monitor the OEs for compliance with AML/CFT obligations (MLTFPA, §64(1)(3)(4)). DMPSs which are carrying out certain activities (see R.1.6) are excluded from the AML/CFT obligations and, therefore, not subject to monitoring compliance with AML/CFT requirements (MLTFPA, §2(1)6)). The designated supervisors for monitoring the compliance with the TFS obligations of the lawyers and notaries are the BA and the MoJ pursuant to the ISA, although in practice, the TFS supervision of notaries is carried out by the CN (ISA, §30(4)(5))[291]. Other DNFBPs are subject to state supervision carried out by the EFIU over the application of TFS by natural and legal persons, as they are not included under the list of *persons with special obligations*[292] (ISA, §30(1), §20(1)).

506. ***Criterion 28.4*** (a) Designated supervisors of the covered DNFBPs have adequate powers to perform their supervisory functions, including the right to inspect, to demand any required information/ documents and receive oral and written explanations from the OEs (MLTFPA, §66).

507. (b) *CSPs and DPMSs:* the same preventive measures which are in place for the FIs under the EFIU's supervision described under c.27.3 are applicable here.

508. The measures to prevent criminals from being professionally accredited, which are at the disposal of the Oversight Board of Auditors, include the assessment of the applicant's good reputation and reliability (AAA, §23(2)2); §39(2)). The repute or reliability shall be deemed to be damaged in the case of a person: i) who has been convicted for an intentionally committed criminal offence; ii) who is subject to the prohibition on business or who has been deprived of the rights to engage in an economic activity; or iii) whose previous unlawful act or omission has resulted in the bankruptcy or revocation of the activity licence of a company. The provisions to not cover the association with criminals. The Oversight Board has the right to revoke the activity licence and the reasons for the revocation include a conviction for an economic criminal offence, criminal official misconduct, criminal offence against property or against public trust (AAA, §87(4)3)).

509. In order to become a notary, a notary candidate must meet the requirement of honesty and *high moral character* (NA, §6(1)). The *unfit* criteria include as well: i) a conviction of a criminal offence; ii) removal from the office of judge, notary or bailiff; and iii) release from the public service for a disciplinary offence (NA, §6(2); CA, §47(2)). The CN may suspend the period office of a notary in case of criminal chargers and the Minister of Justice shall remove a notary from the office in the case of a conviction for an intentionally committed criminal offence, or any other conviction which makes it impossible for the notary to act as a notary (NA, §17(2), §18(3)4)). The measures in place do not ensure that criminals' associates are not licensed.

510. Similar fit and proper checks are in place for attorneys: honesty and ethical requirements; a conviction of an intentional criminal offence; deprivation of the rights to be an attorney, judge, prosecutor, notary or entrepreneur; disbarment or removal from the notary practice (BAA, §23,

[291] Unlike the AML/CFT supervision, the transfer of competences for TFS supervision from the MoJ to the CN is not provided by the legislation, although carried out in practice by the CN.
[292] Credit institutions, financial institutions, VASPs, branches of foreign service providers.

§27(1)). An attorney shall be disbarred in the case of conviction for an intentionally committed criminal offence, or for another criminal offence that renders practicing as an attorney impossible (BAA, §37(2)). The checks do not extend to the association with criminals.

511. Real estate agents, accountants and tax consultants are not subject to professional accreditation.

512. (c) Designated supervisors of the covered DNFBPs, including SRBs, have sanctions available in line with R.35 to deal with non-compliance with AML/CFT requirements. Further details on the available sanctions can be found under R.35. The identified shortcomings under R.35, particularly in relation to the sanctions applied pursuant to the misdemeanour procedure, apply.

513. ***Criterion 28.5*** – The supervisory approach of the EFIU for the FIs described under R.26.5 equally applies to the covered DNFBPs.

514. The administrative supervision of notaries carried out by the CN is based on periodical inspections, which are planned annually. Additional inspections are allowed only in justified cases, where there is a reason to believe that there are significant deficiencies in the notary's activities which need to be quickly eliminated (NA, §5(4); Notarial Regulation, §75(1), §77(3)). Although not risk-based, the planed supervisory activities of CN, pursuant to the annual inspection plans, must take into account some risk-related elements, *inter alia,* the number of notarial acts and complaints lodged against a notary (Procedure for Administrative Supervision of the CN, §2.2 4); Rules of Procedure and Internal Control Rules provided by the MLTFPA and the ISA, §1.8-1.9). As explained by the authorities, this would include the value of the transactions and the type of the transaction, e.g., real estate.

515. The BA does not undertake a risk-based supervision regime, but rather is caring out its inspections applying a random sample.

Weighting and Conclusion

516. A combination of the following is considered to present moderate shortcomings: i) the measures applied by the Oversight Board of Auditors, CN and the BA in order to prevent criminals from owning, managing or operating a DNFBP do not extend to criminals' associates; ii) the power of the EFIU to apply sanctions to deal with failure to comply with AML/CFT requirements is affected by the shortcomings identified under R.35, particularly regarding the sanctions applied pursuant to the misdemeanour procedure; iii) the supervision carried out by the CN and BA is not performed on a risk-sensitive basis; iv) it is not clear how the RBA model of the EFIU takes into account the degree of discretion allowed to the covered DNFBPs under the risk-based approach; v) shortcomings underlined under the conclusion to R. 22 with regard to the scope of application of the MLTFPA, and consequently regulation and supervision, are also relevant here. **R.28 is rated as PCs.**

Recommendation 29 – Financial intelligence units

517. In the 4th round MER of 2014, Estonia was rated LC with the former R.26. The AT noted the insufficient power to query all relevant additional information from lawyers and the confidentiality risk when querying unregulated persons.

518. ***Criterion 29.1 –*** The FIU is the national centre for the receipt and analysis of STRs and other information relevant to ML and TF, and dissemination of information (MLTFPA, §54(1)1). This definition limits the mandate of the EFIU not also extending to dealing with ML predicate offences,

and dissemination of results of its analysis. While the legislation defined the STR in a wider manner, referring to ML, TF and related offences, the duties of the FIU are defined in a narrower manner as dealing with "information referring to ML and TF". While the legislation is precise on dissemination of information held with the FIU, it is not clear on dissemination of the results of the FIU analysis. This is a minor deficiency, which did not materialise in practice during the assessment period.

519. ***Criterion 29.2*** – (a) The FIU serves as the central agency for the receipt of STRs (STRs on ML and TFRs of TF suspicion) from OEs (MLTFPA, §49(1)).

520. (b) The FIU serves as the central agency for the receipt of cash transaction reports (CTRs) for transactions over EUR 32 000 or equal sum in another currency (MLTFPA, §49(2)).

521. In addition, the FIU also receives Unusual Transaction Reports (UTRs), Unusual Activity Reports (UARs), and Unusual Transactions with High-Risk Countries Reports (TR_UAR) (FIU Guidelines on the characteristics of suspicious transactions).

522. ***Criterion 29.3*** – (a) To perform its functions, the FIU has competence to request information from OEs on the basis of a precept (MLTFPA, §58(1)).

523. (b) The FIU has the authority to request any information necessary to perform its functions from competent supervisory authorities, other state authorities, local authority agencies and third parties (on the basis of a precept) (MLTFPA, §58(1)). The FIU has the right to receive information from the bank account register through the electronic seizure system (MLTFPA, §58(1.1)), and obtain data collected by covert operations and cover co-operation from any respective state authority (MLTFPA, §58(3)). The FIU has also can make enquiries to and to receive data from state and municipal databases and databases maintained by persons in public law (MLTFPA, §59).

524. ***Criterion 29.4*** – (a) The FIU should conduct operational analysis, using available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, ML, TF and predicate offences (MLTFPA, §54(1)1).

525. (b) The FIU should conduct strategic analyses that considers the risks, threats, trends and ways of operation of ML and TF (MLTFPA, §54(1)2). When performing this task, the FIU has access to all relevant data, including police intelligence, commercial databases, etc.

526. ***Criterion 29.5*** – The FIU should cooperate with investigative bodies on AML/CFT mattes (MLTFPA, §54(1)6). Duties of the FIU include dissemination of information on ML and TF (MLTFPA, §54(1)2). The FIU should disseminate "the data registered with [it]" to the pre-trial authority, the Prosecutor and the Court upon written request or on the initiative of the FIU (MLTFPA, §60(3)). While the legislation is precise on dissemination of information held with the FIU, it is not clear on dissemination of the results of the FIU analysis.

527. The FIU is using a secure document management system for disseminating materials to the LEA. According to Public Information Act (§ 49^9 (5) exchange of data with the databases belonging to the state information system and between the databases belonging to the state information system shall be carried out through the data exchange layer (X-Road) of the state information system. The EFIU uses a document management system (Delta) in which all incoming and outgoing letters of the EFIU, disseminations (including criminal notices), precepts to obligated persons, and so on are registered and processed. In some cases, EFIU also shares information by entering it directly into the Police database. The Police database is created on the basis of § 8 of

the Police and Border Guard Act and also belongs to the databases belonging to the state information system.

528. ***Criterion 29.6*** – (a) The FIU database is part of the IT system of the State. This system processes the data related to the operations and proceedings arising from the functions of the FIU. Both the MLTFPA and the General Regulation of the Database of the Financial Intelligence Unit, issued by the Minister of Finance, govern access to and the confidentiality of the information contained in the database general rules for handling, storing and protecting information in the EFIU database (MLTFPA, §59.1).

529. (b) All employees of the FIU are assessed before they are employed, a process which includes checking their identities against all the relevant databases, including all police databases. If and when the employee has access to state secrets, the ISS will make an additional assessment. All the analysts in the FIU have EU Restricted level access clearance. The rules stipulated in State Secrets and Classified Information of Foreign States Act and in the subordinated regulations set the parameters and conditions for granting the rights and later supervision. The employees who require access to the Police information database (which contains also criminal intelligence) have separate training by a local contact person and they have to pass the tests before getting access to that database. The employees have to sign a document which attests that they have read, understood and follow data protection regulations. Among else all recruits are introduced with the data protection regulations, the Advisor to the FIU has individual discussions with the new recruits regarding the data protection and the confidentiality obligation and restrictions on use of data (among else banking and business secrecy) as also stipulated in MLTFPA (§60). All the new employees get the individual training regarding the FIU core database RABIS and this will be conducted by an experienced mentor.

530. Disclosure of information obtained in the performance of professional activities by a person required by law to keep such information confidential is an act that is punishable under the Penal Code (§157 and §377).

531. (c) The FIU's premises are accessible to FIU personnel only. The premises are protected with a key card and additional code lock protection. The FIU premises have several surveillance systems and all the systems are password protected.

532. Access to the database is restricted to employees of the FIU but with the permission of the Head of the FIU persons whose involvement is required to perform the duties of the FIU may be granted temporary access to data required for performing the duty to the sufficient extent (MLTFPA, §60 and §62).

533. ***Criterion 29.7*** – (a) The FIU appears to be operationally independent and autonomous. It decides whether to analyse, request and/or forward or disseminate specific information.

534. At the domestic level, under the MLTFPA, the FIU has the right to receive information from the competent supervisory authorities, other state authorities and local authority agencies and, based on a precept, from obliged entities and third parties (Section 58). It is the FIU itself that issues the precepts (Section 55). The FIU also has the right to obtain relevant information, including information collected by surveillance, from any surveillance agency. Where the FIU wishes to forward information collected by surveillance to other authorities, the Financial Intelligence Unit must obtain written consent from the agency which provided the information

(Section 58). Moreover, the FIU also has the right to make enquiries to and receive data from state and local government databases and databases maintained by persons in public law (Section 59).

535. At the international level, Section 63 of the MLTFPA establishes that the FIU has the right to exchange information and conclude cooperation agreements with a foreign authority that performs the duties of a financial intelligence unit or a foreign law enforcement or supervisory agency as well as with an international organisation or institution. The FIU has the right, on its own initiative or upon request, to send and receive to and from another financial intelligence unit any information that the other financial intelligence unit may need in AML/CFT efforts and in processing or analysing information relating to natural or legal persons involved in money laundering or terrorist financing.

536. (b) As noted above, the MLTFPA provides that the FIU may cooperate with a number of domestic authorities in the furtherance of its duties. There is no requirement to conclude MOUs, but the FIU has the right to arrange cooperation agreements with a foreign FIU or law enforcement agency (MLTFPA, §63).

537. (c) the FIU is an independent institution within the jurisdiction of the Ministry of Finance. The FIU has distinct core functions which are regulated by the MLTFPA (Chapter 6).

538. (d) Article 53 of the MLTFPA provides that the FIU is a governmental authority within the Ministry of Finance which is autonomously engaged in regulatory enforcement and autonomously exercises the enforcement powers of the state on the grounds and to the extent provided for in the MLTFPA. The FIU independently performs its tasks under the MLTFPA and independently makes decisions concerning the actions provided for in the MLTFPA. The costs of the FIU are covered by the state budget. The FIU has its own budget that is approved and revised by the Minister of Finance on a proposal of the head of the FIU in accordance with the statutory procedure. The Minister of Finance oversees the FIU's adherence to the budget. Moreover, Section 69 of the MLTFPA provides that internal oversight is not exercised over the FIU as regards the performance of the tasks imposed on the FIU in the MLTFPA and the ISA or the exercise of the rights provided for in these statutes or the preparation and approval of internal orders, instructions and instruments of the FIU in relation to the exercises of these rights or to decisions concerning the service relationships of the officials of the FIU.

539. ***Criterion 29.8 –*** The FIU is a member of the Egmont Group since 16 May 2000.

Weighting and Conclusion

540. The EFIU is provided with all the critical powers and performance of its cove functions. It also has all the requisites in place with regard to operational independence and autonomy. The only minor shortcoming is related to the lack of explicit responsibility for the EFIU to disseminate the results of its analysis. **R.29 is rated as LC.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

541. In the 4th round MER of 2014, Estonia was rated C on former R.27.

542. ***Criterion 30.1*** – In Estonia, the designated LEAs that have responsibility to investigate ML and associated predicate offences are: the PBGB, the ETCB, the Competition Board, the Military Police, the Environment Board, as well as the MoJ's Prisons Department, (CCP, §31). Furthermore,

the designated LEA to investigate TF is the ISS (Regulation no 60293, §2). ML and all predicate offences investigations are conducted by a PBGB, except environmental offences for which Environment Board are competent and ETCB regarding tax and customs crimes and related ML. The ISS is empowered to conduct criminal investigation for TF offence, as well as ML when associated predicate offence is corruption.

543. The PO shall direct criminal investigation and ensure the legality and efficiency thereof, and it has various competences which provide it with an active and supervisory role in the investigative stage (CCP, §30 and §213).

544. ***Criterion 30.2*** – The PBGB, ETCB and ISS are competent to pursue parallel financial investigation and based on the results are obliged to, whenever there is a reasonable suspicion, further investigate ML/TF offence, regardless of where the predicate crime occurred. This obligation comes from the general principle of the CCP (CCP, §6).

545. ***Criterion 30.3*** – The LEAs are empowered to identify, trace and initiate seizure of property that is subject to confiscation or may represent proceeds of crime. Furthermore, the prosecutor is entitled to propose seizure order to the investigative judge (CCP, §142) or in urgent cases can order seizure and later inform the court (CCP, §142(3)).

546. ***Criterion 30.4*** – Not applicable because there are no competent authorities, which are not LEAs, with responsibility for pursuing financial investigations of predicate offences.

547. ***Criterion 30.5*** – According to the authorities, the PBGB and ISS are obliged to investigate corruption offences (within the former there is the Corruption Crime Bureau), and both the PBGB and ISS have competencies for investigating ML/TF. They each have sufficient powers to identify, trace and initiate seizing of property.

Weighting and Conclusion

548. **R.30 is rated C.**

Recommendation 31 – Powers of law enforcement and investigative authorities

549. In the 4th round MER of 2014, Estonia was rated C in former R.28.

550. ***Criterion 31.1*** – The CPC contains a range of measures to enable LEAs and prosecutors to obtain access to documents and other information which are used in ML/TF and related predicate offences investigations.

551. (a) *Production of records:* An investigative body has the right to demand submission of any document necessary for solving a criminal matter (CCP §32) and orders and demands issued by LEAs and PO are "binding on everyone and shall be complied with throughout the territory of the Republic of Estonia" (CCP, §215). Non-compliance with the request is subject to fine imposed by investigative judge (CCP, §215(3)).

552. (b) *Search of persons and premises:* Search may be conducted at the request of the PO on the basis of an order of a preliminary investigation judge or on the basis of a court order, the objective of which is to find an object to be confiscated or used as physical evidence, an object necessary

[293] Regulation Investigative jurisdiction between the Police and Border Guard Board and the Estonian Internal Security Service

for resolving a criminal matter, assets to be seized, a body, or to apprehend a fugitive (CCP, §91). In addition, there is a possibility for physical examination of the person if there are facts that can be used as evidence in the criminal matter (CCP § 88 (1(5))).

553. (c) *Taking witness statements:* During the pre-trial procedure, a body conducting proceedings may require a witness to provide written answers to questions (CCP, §69.2), and there is also provision for tele-hearing (CCP, §69) and depositions of testimony (CCP, §69.1).

554. (d) *Seizing and obtaining evidence:* The LEAs and PO have the power to seize and obtain evidence (CCP, §91), including postal/telegraphic items (CCP §89) powers to make enquiries to electronic communications undertakings for data (CCP, §91.1).

555. ***Criterion 31.2*** – In Estonia, range of investigative techniques are available and include: covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things, covert examination of postal items, wiretapping or covert observation of information, staging of criminal offence, and use of police agents (CCP, §126^{1}-126^{17}). The list of offences upon which surveillance may be carried out includes ML, associated predicate offence and TF offence (CCP, §126^{2}(2)).

556. ***Criterion 31.3*** – (a) *Mechanisms to identify if persons hold/control accounts:* LEAs and PO have the power to obtain financial information including information from the Bank Account Register (see c.31.1).

557. (b) *Mechanisms to identify assets without prior notice to owner:* In Estonia, when identifying assets, there is no requirement to notify the owner of an ongoing investigation, and rather the obligations to disclose the file are only engaged once the investigation stage is complete. Otherwise, information on pre-trial proceedings may be disclosed only with the permission and to the extent determined by the PO, and under conditions that the disclosure of information does not promote criminal activity or complicate the detection of criminal offences (CCP, §214).

558. ***Criterion 31.4*** – Competent authorities when investigating ML, associated predicate offences or TF are able to cooperate with the EFIU (MLTFPA, §54(1)(6)). Furthermore, LEAs and PO have the right to demand from all authorities the submission of a document required for the resolution of a criminal investigation (CCP, § 32) and there is a legal obligation to comply with such request (CCP, § 215).

Weighting and Conclusion

559. **R.31 is rated C.**

Recommendation 32 – Cash Couriers

560. In the 4th round MER of 2014, Estonia was rated LC on former SR. IX. It was noted that the maximum range of sanctions was low particularly in comparison with other EU countries.

561. Estonia is the EU Member State and applies a supra-national approach such that the declaration system for cash and BNIs applies to movements crossing the EU border, and not intra-EU movements.

562. ***Criterion 32.1*** – Estonia applies a declaration system for transportation of cash and BNI entering or leaving EU. For persons, EU Regulation 2018/1672 is directly applicable, which requires, under Article 3, carriers of cash of a value of EUR 10 000 or more to declare that cash to the competent authorities of the MS through which they are entering or leaving the EU and make it available to them for control. Such obligation is not deemed to be fulfilled if the information

provided is incomplete or if the cash is not made available for control. "Cash" is defined in Section 1 of the Regulation to mean currency, bearer-negotiable instruments, commodities used as highly liquid stores of value and prepaid cards.

563. There is no declaration system in place for persons leaving to or entering from another EU Member State, which is a deficiency.

564. As for mail and cargo, whilst Article 4 of EU Regulation 2018/1672 requires the sender or recipient of the cash to make a declaration when cash or BNI valued above EUR 10 000 entering or leaving EU borders, such system does not exist when leaving to or entering from another EU Member State.

565. ***Criterion 32.2*** – All persons entering or leaving EU through Estonia and carrying currency and BNI of EUR 10,000 or more are required to make a truthful declaration, in writing using a paper declaration form or by means of an electronic cash declaration system (EU 2018/1672 and Customs Act, §69).

566. ***Criterion 32.3*** – Not applicable.

567. ***Criterion 32.4*** – In Estonia, according to the authorities, customs officials can seek additional information from passengers upon discovery of a false declaration. Estonia asserts that it relies on the powers under § 30-35 the Law Enforcement Act which apply to customs officers and include stop and question, requiring presentation of documents, summons, compelled attendance, establishment of identity and use of monitoring equipment which forwards images or records. Furthermore, §44-52 of the Law Enforcement Act provide further special state supervision measures which the ETCB may exercise (prohibition on stay, stopping of vehicle, detention of person, security check, examination of persons/premises/movables, and entry into premises).

568. ***Criterion 32.5*** – The sanctions applied for false declaration depend on the character of the violation. Criminal proceedings are initiated if the cash or BNI exceeds EUR 40 000 (Penal Code, §391); and misdemeanours are initiated in all other cases (Customs Act, §69).

569. *Criminal proceedings:* §391 of the Penal Code provides that inter alia a failure to declare goods or cash, use of a false description or use of any other fraud while carrying cash to be declared across the frontier of the customs territory of the EU, is punishable by a pecuniary sanction or up to four years' imprisonment. For an official taking advantage of his or her official position there is no pecuniary punishment, and the maximum imprisonment is 5 years. For a legal person the sanction is a pecuniary punishment (see R.3 for details on the calculation and maximum size of the pecuniary punishments).

570. *Misdemeanour proceedings:* for natural persons, the conveyance of goods or cash subject to declaration from across the EU border by evading customs controls, failing to declare the goods or cash, declaring the goods or cash under an incorrect tariff classification or description, or behaving in any other fraudulent manner is punishable by a fine of up to EUR 1 200 or court may impose detention for a term of up to 30 days (Penal Code, §47 and §48) .

571. ***Criterion 32.6*** – The competent authorities shall transmit to the EFIU the information recorded for false or failed disclosures (EU Regulation 2018/1672, Art.9). According to the authorities, the ETCB forwards, at least once a month, a detailed report from its database with the metadata of all cross-border cash delivery declarations to the EFIU. The EFIU uses the data for risk monitoring and analysis. The ETCB also files an STR via the electronic reporting system to

the EFIU if they detect illegal cross-border cash delivery. The EFIU will analyse the report and take necessary measures if there is a need to stop the movement of property.

572. If the ETCB considers any cash transportation suspicious or for all declarations exceeding EUR 10 000, the EFIU is said to be always informed, according to cooperation Agreement.

573. ***Criterion 32.7*** – The cash declaration system is now connected to the EFIU information system, and therefore there is strong co-operation with the EFIU. In addition, the EFIU and ETCB have signed an agreement of co-operation as regards cash declarations and related issues. The ETCB has mutual co-operation with other competent authorities such as the PBGB and ISS.

574. ***Criterion 32.8*** – Pursuant to the EU Regulation 2018/1672 (Art.7) and the Customs Act (§66[1]), the customs authorities have the right to temporarily detain cash for up to three business days. This power is not constrained by purpose requirements so implicitly includes where there is a suspicion of ML/TF and where there is a false declaration.

575. ***Criterion 32.9*** – Authorities cooperate with foreign counterparts (EU Member States and the third countries) following the terms established pursuant to EU Regulation 2018/1672 (Art.10 and Art.11). These provisions require the exchange of information regarding declarations of above EUR 10 000, false declaration or where there is suspicion of criminal activity. Information obtained from cash declarations is retained and recorded in the Cash Declaration System) and available for both domestic and international co-operation.

576. ***Criterion 32.10*** – As the EU Member State, Estonia shall apply safeguards to the personal data privacy as stipulated in the EU Regulation 2018/1672 (Art.12 and Art.13).

577. ***Criterion 32.11*** – (a) Persons carrying out physical cross-border transportation of currency or BNIs related to ML/TF or predicate offences would be liable to prosecution under the ancillary offences under the Penal Code (§22, §221, §25), with the associated proportionate and dissuasive sanctions available as detailed in R.3 and R.5.

578. (b) The ETCB having conducted extra-judicial proceedings may confiscate an object or substance which has been the direct object of commission of a misdemeanour provided for in the Customs Act (§69-72). Furthermore, the Penal Code (§83, §83[1], and §84) could apply and the currency/BNI could be confiscated.

Weighting and Conclusion

579. Estonia achieves compliance with the majority of criteria of this Recommendation. However, there is no EU-internal border declaration system for cash or BNIs through mail and cargo. This meaning that, overall, the shortcomings are minor. **R.32 is rated LC.**

Recommendation 33 – Statistics

580. In the 4th round MER of 2014, Estonia was rated as LC on former R.32.

581. ***Criterion 33.1*** – *(a) STRs (received and disseminated):* all STRs received by the EFIU are registered in the EFIU's information system which also includes in its meta data the information about reports disseminated (MLTFPA, §54(1)(1)).

582. *(b) ML/TF investigations, prosecutions and convictions:* Authorities advised that MoJ keeps statistics on the number of ML/TF investigations, prosecutions and convictions, regardless of the source of the investigation. However, there is no comprehensive statistics kept by the authorities

such as ML investigation per predicate crime, ML investigation triggered by different type of information, ML prosecution per predicate crime.

583. (*c) Property frozen, seized and confiscated*: Authorities advised that the PGO collects statistics regarding property seized and confiscated. However, there is no comprehensive statistics that is provided regarding property seized and confiscated. This problem is also recognised by Estonia in its latest NRA from 2021. There is no statistics on the seized and confiscated instrumentalities, restitutions to victims, division between confiscation from domestic and foreign predicates, extended confiscation, assets recovered, sharing of assets with foreign countries.

584. *(d) MLA and other international co-operation requests for co-operation made and received:* In Estonia, according to provided information, the OPG collects statistics on MLA, both incoming and outgoing requests. However, there is a missing data for number of years on the status of the received requests and, therefore, it cannot be concluded that comprehensive statistics is kept. In addition, all LEAs do not keep statistics on the other forms of international cooperation on the AML/CFT matters.

Weighting and Conclusion

585. In Estonia, the EFIU is obliged to maintain statistics on STRs, received and disseminated. However, there is no comprehensive statistics maintained on: ML/TF investigations, prosecutions, and convictions; on property seized and confiscated; as well as on the MLA and other forms of international cooperation. **R.33 is rated PC.**

Recommendation 34 – Guidance and feedback

586. In the 4th round MER of 2014, Estonia was rated C with former R.25.

587. ***Criterion 34.1*** – The EFIU has published on its website[294] four guidelines that reflect on the characteristics of reports; the reporting obligation; on the management of risks relating to ML/TF and application of due diligence; implementation of financial sanctions.

588. The authorities advise that, since 2020, the EFIU established the practice of providing annual written feedback to OEs by sending individual feedback to the eight largest reporting entities. In addition, sectoral feedback reports for VASPs, FIs, real estate agents, DPMSs and the gambling operators were prepared and circulated to the OEs. In 2021, the EFIU provided individual feedback to 10 OEs and published sector-based feedback reports[295].

589. Regarding feedback on STRs, the EFIU advises of providing individual feedback to the OE in the preliminary analysis stage, upon identifying inconsistencies in the report. Thereafter, the OE has an opportunity to send additional information and materials. At the same time, it may adjust the internal processes as per the instructions of the EFIU. Where the STR is marked as urgent, the preliminary analyst would also provide feedback to the OE regarding issuance of a precept to suspend transactions. There is, however, no guidance provided on TF-specific typologies and schemes, especially to the sectors with higher exposure to risks.

590. The EFSA has developed and published its supervisory policy setting out the expectations regarding market participants, particularly defining that FIs, and especially systemically important market participants must apply appropriate systems and controls to ensure

[294] Available at https://fiu.ee/en/guidelines-fiu/guidelines
[295] Available at https://fiu.ee/aastaraamatud-ja-uuringud/tagasiside-teatajatele

compliance with AML/CFT requirements. In 2018, a new advisory manual has been published to guide financial intermediaries on organisational solutions and preventive measures to combat ML/TF. This manual provides the details on how to identify, understand and analyse threats and how to manage them. In 2021 the EFSA developed and published the Guideline on implementation of financial sanctions, addressed to its supervised OEs. The EFSA conducted the annual information days for all financial sectors held on 7-9 December 2021.

591. The CN and the BA have issued guidance for ML/TF risk assessment, as well as rules of procedure and internal control rules for mitigation and management of ML/TF risks.

Weighting and Conclusion

Overall, all OEs are provided, to a varying extent, with guidelines and feedback, but no guidance is provided on TF-specific typologies and schemes, especially to the sectors with higher risk exposure. **R.34 is rated LC.**

Recommendation 35 – Sanctions

592. In the 4th round MER of 2014, Estonia was rated PC on former R.17. The report noted that the range of available sanctions was neither effective, nor proportionate for certain categories of financial institutions, the maximum financial penalties did not appear dissuasive, the sanctions available for legal persons that are financial institutions were not available for their directors and senior management, and that the sanctions applied in practice were of a narrow range.

593. R.10 and R.22 lists activities to which the MLTFPA does not apply and so which are not subject to regulation or supervision.

594. ***Criterion 35.1*** – Non-compliance or improper compliance by individuals and legal persons with obligations under MLTFPA and ISA is subject to administrative measures, fines imposed pursuant to the misdemeanour proceedings, disciplinary penalties and criminal sanctions (in case of unlicensed economic activity).

R.9 to 23 - FIs, DNFBPs

Administrative measures

595. The EFSA and the EFIU have powers to issue a precept for covered FIs and covered DNFBPs (except for notaries and lawyers), which is a statutory mean to prescribe an obligation, e.g., to preclude to provide specific services, to terminate an employment contract with an employee, to recall a member of a management board, or to make other demands.

596. Failure to comply or improper compliance, by an OE, with an administrative decision (precept) issued by the EFSA or the EFIU, determine the right of the two supervisory authorities to impose coercive measures in the form of a non-compliance levy, i.e., a penalty payment (MLTFPA, §65; FSAA, §18(2)4), §55(1)). The maximum non-compliance levy which can be applied by the EFIU for the first non-compliant act committed by an FI pursuant to the issued precept is: (i) up to EUR 5 000 in case of a natural person; and (ii) up to EUR 32 000 in the case of a legal person. It can be increased on any subsequent occasion up to EUR 50 000, respectively EUR 100 000, but not more than EUR 5 000000 in total for natural person and EUR 5 mil or 10% of the total annual turnover, for legal persons (MLTFPA, §65(2)). The maximum of the non-compliance levy which can be imposed by the EFIU in case of VASPs and DNFBPs is significantly lower: i) up to EUR 5 000 in the case of a natural person; and ii) up to EUR 32 000 in the case of a legal person (MLTFPA, §65(4)). In the case of VASPs, the maximum non-compliance levy is not

considered to be sufficiently dissuasive.

597. The powers of the EFSA to impose a non-compliance levy are established by the sectoral legislation and the upper limits vary depending on the sector:

Table 1. Maximum limits of the non-compliance levy, which can be imposed by the EFSA

Sector	Subject	Upper limit for the first occasion (EUR)	Upper limit for the subsequent cases (EUR)	Total highest limit (EUR)
Credit institutions (CIA, §104[1])	Natural person	5 000	50 000	5 000 000
	Legal person	32 000 000	100 000	≤ 10% of the net annual turnover
Creditors and credit intermediaries (CCIA, §95)	Natural person	1 200	n/a	6 000*
	Legal person	3 200	n/a	52 000*
PSPs and EMIs (PIEIA, §106)	Natural person	1 200	n/a	6 000*
	Legal person	3 200	n/a	52 000*
Investment firms (SMA, §§ 234[1])	Natural person	5 000	50 000	5 000 000[296]
	Legal person	32 000 000	100 000	15 000 000 or ≤ 15% of the total annual turnover[297]
Fund managers (IFA, §463)	Natural person	5 000	50 000	5 000 000
	Legal person	32 000 000	100 000	≤ 10% of the net annual turnover
Insurance firms (IAA, §238)	Natural person	5 000	50 000	5 000 000
	Legal person	32 000 000	100 000	5 000 000 or ≤ 10% of the total annual turnover[298]

* Highest limit for the non-compliance with the same obligation

598. As illustrated by the Table above, the powers of the EFSA to impose a non-compliance levy, including the maximum limits, are very similar to those of the EFIU for the majority of the sectors under its supervision. Nevertheless, in the case of PSPs, EMIs and credit providers, the powers are significantly more limited compared to those of the EFIU in relation to the FIs under its supervision and, therefore, cannot be considered as having an effective, proportionate or dissuasive character.

Financial penalties under misdemeanour proceedings

599. The EFIU and the EFSA also have powers to act as the out-of-court (misdemeanour) proceeding authorities (MLTFPA, §97). Chapter 10 of the MLTFPA outlines the misdemeanours and appears to cover all failings under the MLTFPA. The maximum fine which can be imposed based on the misdemeanour proceedings, per violation, is up to EUR 1 200 for natural persons and EUR 400 000, for legal persons (MLTFPA, Chapter 10; PC, §63(3)). Both, intentional and negligent acts are punishable as misdemeanours (PC, §15 (3)). The decisions of the EFSA and EFIU, taken as extra-judicial bodies, cab be appealed in court (CMP, §19 7)). A fine up to EUR 1 200 for natural persons and up to EUR 400 000 is not considered by the AT as dissuasive and, likewise, is not perceived by the authorities as an effective deterrent for an AML/CFT breach. In this respect, the country has informed about a legislative initiative to address this shortcoming - two legislative bills have been presented to the Parliament which aim to increase the

[296] or up to three times the amount of the profits gained, or losses avoided as a result of the violation if such profits or losses can be determined.
[297] or up to three times the amount of the profits gained, or losses avoided as a result of the violation if such profits or losses can be determined.
[298] or up to double amount of the profits gained, or losses avoided as a result of the violation if such profits or losses can be determined.

misdemeanour fines up to 20 000 000 euros, up to 15% of the turnover of the legal person or two to three times profits earned, or losses avoided with the infringement.

600. Pursuant to the Penal Code, a misdemeanour constitutes a minor offence. The collection of evidence and the procedural operations under the misdemeanour procedure are subject to the provisions of criminal procedure (CMC, §31(1). This calls for an evidentiary standard comparable to that required under criminal proceedings, although under the condition of a more restricted limitation period, compared to that established for criminal offences. Moreover, not in all cases the evidence collected during the administrative supervisory procedure can be used in misdemeanour procedure, e.g., testimonies, and the authorities are required to "re-collect" such evidence. The limitation period for a misdemeanour related to a violation of the AML/CFT obligations is two years, calculated as of the completion of the violation, the completion of the last act (in case of intermittent offences), or as of the termination of the contiguous act (in the case of a continuous offence) (PC, §83(3)(4)). The limitation period is interrupted upon commencement of criminal proceedings in a matter of an act with elements of misdemeanour, until the termination of the criminal proceedings, but cannot be resumed if more than 3 years have passed from the completion of the misdemeanour (PC, §81(7)2), (8)). Considering the duration of criminal investigations/ trial, it can be reasonably presumed that in most of the cases, when there is an unsuccessful criminal investigation/ conviction, the misdemeanour procedure would not be resumed due to the expiration of the limitation period. This aspect, together with the above mentioned evidentiary and procedural requirements, as well as the low maximum amount of fines that can be imposed, lead to the conclusion that the financial penalty under misdemeanour proceedings does not feature the characteristics of an effective, proportionate and dissuasive sanction.

601. The final decisions made in a misdemeanour case, as well as the final administrative decisions, including on the imposition of non-compliance levy, taken by the EFSA and EFIU, must be published without delay, subject to some exemptions due to justified circumstances, which give the right to the authorities to postpone or not to publish the final decisions (MLTFPA, §67(3)-(5)). This requirement is recognised to be an effective deterrent to those entities to whom a potential reputational impact is a more material consideration than monetary sanctions.

Detention under misdemeanour proceedings

602. A court may impose detention for a term of up to 30 days for a misdemeanour (PC, §48). A district court would have the competence in such cases (CMP, §83 2)). Chapter 10 of the MLTFPA provides for the possibility to impose detention on a natural person when there is a breach of the key obligations under the MLTFPA, such as: i) the duty to identify and verify the person's identity; ii) the duty to identity the BO; iii) the duty to report suspicion of ML/TF; and iii) the duty of confidentiality (MLTFPA, §84(1), §85(1), §92(1) and §93(1)).

Revocation of a licence/ authorisation

603. The powers of the EFIU to revoke an authorisation are provided by §37 (1) of the General Part of the Economic Activities Code Act and §75 of the MLTFPA and can be applied including in cases of repeated fails to follow compliance notices issued by a regulatory enforcement or supervisory authority (MLTFPA, §75(1)2)). The powers of the EFSA are established under the FSAA, §18(2)1), as well as under the relevant sectoral laws – CIA, §17; CCIA, §18; PIEIA, §22; SMA, §58; IFA, §§317-318; IAA, §23. Among the reasons for a full or partial revocation of the authorisation are: i) cases of repeated violations of the provisions of the MLTFPA and ISA; ii) failure to implement a precept within the term or to the extent prescribed; iii) involvement/

commission of ML (CIA, §17(1)12), 14); CCIA, §18(2)14), 17); PIEIA, §22(2)13), 16); SMA, §58(2)6), 9); IFA, §318 11), 13); IAA, §23(1)6), 8)).

604. Regarding casinos, such powers are conferred to the ETCB, based on the GA, §20 and can be applied including in cases of: i) repeated violations of the provisions of the MLTFPA; iii) involvement/ commission of ML; iii) failure to implement a precept within the term or to the extent prescribed (GA, §20(1)7), (2)2)). The same measures can be applied to auditors by the AAOB, based on the powers conferred by the Auditors Activities Act, §20. The real estate agents and accountants are not subject to registration/ licensing requirements. The powers to remove/ disbar a notary/ lawyer are described below under the disciplinary penalties.

Disciplinary penalties

605. Lawyers and notaries are subject to disciplinary penalties, which include: i) a reprimand; ii) a fine in the amount of up to EUR 16 000 and iii) removal from the office/ disbarment (BAA, §19(2); NDLA, §3). In the case of lawyers, additional disciplinary measures can be applied, such as the suspension of the legal practice for up to one year, as well as the revocation of certain activity rights for up to five years. The powers to impose the disciplinary penalties are conferred to the Ethics Tribunal, in the case of lawyers (BAA, §15(1)), and to the MoJ and the court of honour of the CN, in the case of notaries. Only the MoJ is entitled to remove from office a notary (NDLA, §4). The limitation period is three years after the disciplinary offence was committed (BAA, §19(6); NDLA, §7^1(1)). The range of available sanctions, including the maximum amount of fine which can be imposed, appears to be proportionate and dissuasive.

Criminal sanctions

606. Carrying out activities without an activity licence in a field where such activity licence is required is punishable by a fine of up to EUR 1 200 or detention, or up to EUR 5 000 or three years of imprisonment, if the illegal activity concerns providing credit, insurance or financial services, and the act was committed by a natural person. In the case of the legal persons the maximum fine which can be imposed is up to EUR 32 000. When the illegal activities provided by the legal person are related to credit, insurance or financial services, a pecuniary punishment may be imposed, which is calculated on the basis of the average daily income of the offender (PC, §372).

TFS

607. The analysis of the sanctioning regime, under R.7.3, for the non-compliance with the requirements of the R.7 equally applies to cases of non-compliance with the requirements of R.6 and is relevant here.

NPOs

608. See criterion 8.4(b).

609. ***Criterion 35.2*** – The administrative measures described under c.35.1, i.e., precepts, are issued to legal persons. Nevertheless, depending on their scope, they can have a direct an impact or effect on the natural persons, including the directors and senior management of the covered OEs (e.g., when the precept demands the removal of a manager of an OE, or the temporary suspension of his/her authority). The financial penalties pursuant to the misdemeanour proceedings may be imposed to both natural and legal persons, thus being applicable to the directors and senior management of the covered OEs.

Weighting and Conclusion

610. Estonian supervisors have powers to impose a broad range of sanctions for AML/CFT related violations including administrative and disciplinary measures, misdemeanours fines, and criminal sanctions. However, the following moderate shortcomings have been identified in relation to the implementation of R. 35: i) the lower upper limits of the non-compliance levy with respect to PSPs, EMIs and credit providers has impact on the effectiveness, proportionality and dissuasiveness of the available administrative measures; ii) the financial penalty under misdemeanour proceedings does not feature the characteristics of an effective, proportionate and dissuasive sanction; iii) additionally, in relation to the available sanctions for non-compliance with the TFS obligations, the sanctions under the misdemeanour proceedings do not extent to all OEs and do not cover the compliance with obligation to freeze without delay and prior notification (see c.7.3); iv) although subject to sanctions for non-compliance with the AML/CFT requirements, no sanctions are available for the NPOs for the non-compliance with the requirements of R.8; v) shortcomings underlined under the conclusion to R.10 and R.22 with regard to the scope of application of the MLTFPA (and consequently regulation and supervision) are also relevant here. **R.35 is rated PC.**

Recommendation 36 – International instruments

611. In the 4th round MER of 2014, Estonia was rated PC on both former R.35 and SRI. There were doubts whether conviction or at least indictment for the predicate offence is a prerequisite for ML conviction. The TF Convention was not implemented in full.

612. ***Criterion 36.1 –*** Estonia is a party to the Vienna Convention (ratified on 31 May 2000), the Terrorist Financing Convention (ratified on 20 March 2002), the Palermo Convention (ratified on 4 December 2002), and the Merida Convention (ratified on 20 January 2010).

613. ***Criterion 36.2 –*** Estonia has implemented provisions of the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption. However, the International Convention for the Suppression of the Financing of Terrorism has not been fully implemented, since there are deficiencies identified in the incrimination of TF offence (see R.5).

Weighting and Conclusion

614. Estonia implemented all the respective convention. However, there are gaps in implementation of International Convention for the Suppression of the Financing of Terrorism, as described in R.5. Therefore, **R.36 is rated LC.**

Recommendation 37 – Mutual legal assistance

615. In the 4th round MER of 2014, Estonia was rated LC on both former R.36 and SRV. It was noted that the shortcomings of the ML and the TF offences may limit MLA based on dual criminality.

616. ***Criterion 37.1 –*** Estonia can provide MLA based on international treaties and provisions of CCP. There is separate Chapter of the CCP (Chapter 19) which defines different forms of international cooperation in criminal proceedings with EU and non-EU member states such as: extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, cooperation with the International Criminal Court and Eurojust and extradition to Member States of the European Union. This legal basis allows to rapidly provide MLA with respect

to investigation and prosecution of ML, TF and predicate offences, when requested by foreign jurisdictions.

617. ***Criterion 37.2 –*** The MoJ is the central authority responsible for coordination and organisation of judicial cooperation in criminal matters with non-EU countries. The competent authority for receiving European Investigation Orders (EIO) and European Freezing Certificates is the OPG.

618. The Courts, POs, PBGB, the ISS, the ETCB, the Competition Board and the Military Police are the authorities competent to engage in international co-operation in criminal procedure to the extent provided by law (CCP, §435).

619. Timely execution of the MLA request is ensured through the provisions of CCP (§ 436.3). Regarding EIOs deadline for recognition is set to 30 days (CCP, § 489.47). If a request cannot be responded to immediately or within the deadline, the judicial authority of the requesting state should be notified indicating deadline when the response will be provided (CCP, §436.3).

620. In order to ensure monitoring process, the OPG uses a digital management system, for electronic case management. All requests are handled digitally, and the progress is monitored. Basic principles for prioritisation of the requests are envisaged in the written guidelines issued by the OPG.

621. ***Criterion 37.3*** – The grounds for refusals of a request for legal assistance do not pose unreasonable or unduly restrictive conditions (CCP, §436).

622. ***Criterion 37.4*** – (a) Estonian legislation does not envisage refusals of the MLA request if it concerns fiscal offence (CCP, §436). At the same time, it is stated that Estonia shall not refuse to engage in international cooperation with a Member State of the European Union on the ground that the same kind of tax or duty is not imposed, or the same type of taxes, customs or exchange arrangements have not been established in Estonia as in the requesting state (CCP §436(1.2)).

623. (b) Secrecy or confidentiality matters are not included as the mandatory grounds for refusal (CCP, §436).

624. ***Criterion 37.5*** – Confidentiality obligation for MLA is provided to the extent necessary for cooperation. If the confidential information for any reason may be disclosed, the requesting state shall be notified thereof (CCP, § 433(4)).

625. ***Criterion 37.6*** – Estonian authorities state that the legislation (CCP) does not require fulfilment of the dual criminality requirement. However, provision of CCP applies if otherwise is not stated in the international agreements, EU legislation and principles of the international law. In this respect, pursuant to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 030) (Art. 1 and Art.23(1)), Estonia reserved the right to refuse cooperation in case when the request concerns an act which is not considered an offence under Estonian laws. Therefore, even in cases which do not involve coercive measures, authorities can refuse request for assistance based on the principle of dual criminality. This may limit the assistance that country can offer taking into consideration deficiencies identified in incrimination of TF offence (see R.5).

626. ***Criterion 37.7*** – Authorities advised that if the offence by factual circumstances constitutes a criminal offence under the Penal Code of Estonia, MLA shall be delivered regardless of the denomination of the offense in the requesting country. There is nothing in the legislation requiring that the offence described in a foreign country use the same terminology or fall within

the same category of offence. However, the gaps identified in incrimination of TF offence (see R.5) may limit the assistance that the country can offer to non-EU Member States.

627. ***Criterion 37.8 –*** Competent authorities may use all powers available for the investigation of crimes domestically in response to requests for MLA. This includes:

628. (a) all the specific powers required under R.31 relating to the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons, and the taking witness statements (CCP, §433(3))

629. (b) A broad range of other powers and investigative techniques, including the application of surveillance measures (CCP, §433(3))

Weighting and Conclusion

630. Estonia meets most of the criteria under this recommendation. However, application of the principal of dual criminality can limit the ability to provide MLA for TF offence. Therefore, **R.37 is rated LC**.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

631. In the 4th round MER of 2014, Estonia was rated LC on former R.38. Estonia uses the EU and CoE conventions and framework for cooperation and extradition within the EU. Estonia also has signed several bilateral agreements. It appeared that Estonia might fully assist in MLAs and international cooperation and that the only limitations were conflict with the provisions for refusing international cooperation in the CCP (§436).

632. ***Criterion 38.1*** – Estonian authorities can take expeditious actions in response to the request for identification, seizing and confiscation. The legal framework for MLA described in R.37, when cooperating with non-EU Member States, is applicable also regarding MLA for identification, seizing and confiscation of laundered proceeds, proceeds and instrumentalities from ML/TF and predicate offence and property of corresponding value (CCP, §433(3)).

633. Furthermore, Estonian authorities can take actions within the EU Regulation 2018/1805 in regard to identification, seizing and confiscation of laundered property, proceeds, instruments used in a criminal offence and other evidence in ML/TF offences or predicate offences. In addition, assistance in this matter with regard to Denmark and Ireland is provided based on the Framework decision FD 2003/577/JHA.

634. ***Criterion 38.2*** – In Estonia, when request for cooperation from EU Member States is made for non-conviction-based confiscation, authorities can use legal basis provided in EU Regulation 2018/1805 (Article 2(2) and 2(3)(d) on the mutual recognition of seizure and confiscation orders. However, there is no legal basis for providing assistance to non-EU Member States if the request is related to non-conviction-based confiscation.

635. ***Criterion 38.3*** – (a) Estonia has arrangements for coordinating seizure and confiscation. This arrangement can be in the form of JIT or can take place through EUROJUST, CARIN, ARO and EJN networks. In addition, authorities advised there is a liaison officer (*legal attaché*) in the USA with the specific role of enhancing cooperation *inter alia* tracing and recovery of assets.

636. (b) Estonia has domestic mechanisms for managing and disposing of property (CCP, §126) which is applicable when assets are seized or confiscated based on the foreign request. Regarding disposal of assets received upon execution of foreign court judgements, confiscated property shall be transferred to revenues of Estonia unless the parties have agreed otherwise (CCP, §487(2)).

637. ***Criterion 38.4*** – Confiscated property can be shared with other EU countries based on EU Regulation 2018/1805 and Treaty between the Government of the Republic of Estonia and the Government of USA. In addition, the OPG sharing of assets can be agreed based on Article 14 of the United Nations Convention Against Transnational Organized Crime and Article 57 of the United Nations Convention Against Corruption.

Weighting and Conclusion

638. Estonia has met majority of requirements. However, deficiency has been identified in respect to providing assistance in non-conviction-based confiscation matters to non-EU Member States. Therefore, **R.38 is rated LC**.

Recommendation 39 – Extradition

639. In the 4th round MER of 2014, Estonia was rated LC on former R.39. The main deficiency was that the application of dual criminality might create an obstacle to extradition in cases involving TF activities.

640. ***Criterion 39.1*** – Estonia can execute extradition request for the purpose of criminal proceedings or execution of the judgement (CCP, §439-459) without undue delay. The extradition for criminal prosecution or trial is only possible when the corresponding offence is punished by 1 year of imprisonment. Extradition for the execution of a judgement is only possible if the imposed imprisonment penalty exceeds 4 months. As the EU - Member State, Estonia has implemented European Arrest Warrant (CCP, §490-508). In addition, Estonia has ratified European Convention on Extradition and two additional protocols, but not its 3rd and 4th protocols.

641. (a) ML and TF are extraditable offences.

642. (b) There is a case management system used in extradition proceedings. According to the authorities, all incoming and outgoing extradition requests are registered in Delta and the deadlines for timely execution are set in the system. Within Estonia all documents related to extradition are sent electronically through Delta to other competent authorities, as well as to foreign states, when available. The procedure for extradition of person to foreign states is divided into preliminary proceedings in the MoJ and the OPG, verification of the legal admissibility of the extradition in the court, and final decision on extradition falls within the competence of the executive power (CCP, §443).

643. (c) The conditions for the non-execution of requests as defined by the CCP (§440 and §492) do not appear unreasonable or unduly restrictive.

644. ***Criterion 39.2 –*** (a) Estonian Constitution allows extradition of nationals only when it is provided by an international treaty (§36).

645. (b) In Estonia, if nationals are not extradited, upon request of the country seeking extradition, in accordance with the European Convention on Extradition (Art.6(2)), authorities will submit the case without undue delay to the competent authority for prosecution. In such cases reliance is also on the general provision of the Penal Code which states that criminal legislation is applicable to the nationals and foreigners residing in Estonia, who commit crime in a foreign country.

646. ***Criterion 39.3*** – Dual criminality is a requirement for the execution of the extradition request (CCP, §439 and §492). However, no provision in the legislation suggests that crimes must

necessarily fall within the same category of offence or denominate the offence by the same terminology. The fact that both countries criminalise the conduct underlying the offence is sufficient to consider the dual criminality requirement as satisfied. However, deficiencies identified in incrimination of TF offence (see R.5) may limit the possibility of Estonia to execute extradition requests.

647. ***Criterion 39.4*** – Simplified procedure is foreseen for the extraditions of the foreigners both to EU and non-EU Member States. In case of the extradition to non-EU Member State, simplified procedure can be applied, and decision is taken by the MoJ without verification of the legal admissibility of the extradition (CCP, §449). In case of EAW, when person consents with the surrender, a court session shall be held within 5 days as of the receipt of the EAW by a court (CCP, §449 and §502).

648. In case the person doesn't consent to extradition, a regular extradition procedure starts and within 10 days since the receipt of the extradition request a court hearing is organised.

Weighting and Conclusion

649. Estonia meets most of the requirements of the recommendation. However, deficiencies identified in incrimination of the TF offence may limit the execution of the extradition of the foreign request since dual criminality is required. **R.39 is rated LC.**

Recommendation 40 – Other forms of international cooperation

650. In the 4th round MER of 2014, Estonia was rated LC on former R.40. The main deficiencies were lack of information regarding the grounds for refusal and non-execution and that relevant law-enforcement authorities should keep statistics on ML/TF operational cross-border exchanges.

651. ***Criterion 40.1*** – The competent authorities are able to rapidly provide a wide range of cooperation in relation to ML, TF and associated predicate offences, both spontaneously and upon request. (CCP, § 433, §435, §436.3, §473, MLTFPA, §63 (1), Security Authorities Act, §32(3.1) and the FSA Act, §47(1)). The legal basis for cooperation of EFIU in a capacity of a supervisor is undeveloped.

652. The PBGB, the FIU and the ISS, have appropriate mechanisms for exchanging information on daily-based co-operation. When acting in a capacity of a LEA the ISS uses the PBGB cooperation for obtaining information. The ETCB can exchange information concerning VAT, income tax and other relevant information with its counterparts. International cooperation with EU and non-EU members is conducted on the basis of international Conventions, bilateral and multilateral agreements and on the principle of reciprocity. Competent authorities cooperate also through the provision of international networks as the Egmont Group, Europol, EUROJUST, INTERPOL, EPAC/EACN network[299], CARIN network, PWGT[300] and other. The EFSA cooperates with other supervisory authorities based on MoUs, through different working groups such as AML/CFT supervisory colleges, the Nordic-Baltic working Group, and shares information via information exchange platforms set up by the EBA, I.e., EuReCA and E-Gate databases.

[299] European Partners Against Corruption/European Anti-Corruption Network.
[300] Police Working Group on Terrorism

653. ***Criterion 40.2 –*** (a) Competent authorities have their own legal basis for providing international co-operation. The legal base for international co-operation is CCP (§435), MLTFPA (§63)(1)), Security Authorities Act (§32(3.1)) and the FSA Act (§47(1)).

654. (b) There are no impediments for providing and/or requesting co-operation. Nothing prevents authorities from using the most efficient means to cooperate.

655. (c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. The systems are protected and access is restricted. The EFIU uses FIU-net and EGMONT Secure Web. The EFSA the EuReCA and E-Gate databases and the EBA AML Colleges Information Sharing Platform, whereas information and operation security for all of them is guaranteed by the EBA. The PBGB and the ETCB use INTERPOL (I–24/7), EUROPOL (SIENA) and SIS (SIRENE) mechanisms. Additionally, ETCB also uses the European Commission Customs Risk Management System. The ISS uses the secure CT-SIENA platform, accessible only for EU member states CT-units.

656. (d) Competent authorities have processes in place to assess and prioritise requests and ensure timely assistance is provided. The EFIU follows the Egmont Principles for the prioritisation or timely execution of requests. The PBGB case management system supports prioritisation (urgent, ongoing; live data) and timely execution using a colouring system and systematic reminder notices. The PBGB, the ETCB and ISS process the requests within reasonable time frames, in accordance with the rules of priority drawn up by the mechanisms used for information exchange (e.g., INTERPOL or EUROPOL). In addition, international cooperation is facilitated by the network of attachés.

657. (e) Any requirement of confidentiality shall comply with in the course of international co-operation in criminal proceedings to the extent necessary for co-operation (CCP§ 433 (4)). Information received from counterparts is handled in SIENA or criminal intelligence databases and is made available only on a need-to-know basis. All officers related to the international police co-operation and information exchange have the EU RESTRICTED level access clearance, and they undergo regular training. The FIU and the ISS have clear processes for safeguarding the information (MLTFPA §60(1)(8), §63 (1) (8-10)).

658. ***Criterion 40.3 –*** Estonia has international instruments such as multilateral or bilateral instruments in place and also EU instruments. Estonia has also entered direct agreements as well as annual action plans with their closest cross-border partners. There are ten (10) intergovernmental agreements and seven (7) inter-institutional co-operation plans[301] with relevant counterparts. The EFIU has the mandate to negotiate and enter agreements in relation to its duties of cooperation in the scope of AML/CFT (MLTFPA, §53, 63). The ISS has mechanisms as the CT-SIENA for information-sharing with their counterparts, however the details of their co-operation are classified. The EFSA has the mandate to entry into cooperation agreements with

[301] Cooperation Plan of Finnish National Police Board and Estonian Police and Border Guard Board for the year 2021.
Cooperation Plan of North Prefecture of the Estonian Police and Border Guard Board and Helsinki Police Department for the year 2019-2021.
Cooperation Plan between the South Prefecture and East Prefecture of the Estonian Police and Border Guard Board and South- Eastern Finland Police Department for the years 2020- 2021.
Annual Action Plan on Cooperation of Estonian, Latvian and Lithuanian Public Order Police Units for the Year 2021.
Cooperation Plan between the Police of the State of Rhineland-Palatinate and the Estonian Police for the year 2021.
North Prefecture and Riga Region Police Department Action Plan for 2020-2021.
Protocol on Border Guard Cooperation between Police and Border Guard Board of the Republic of Estonia and Federal Security Service of the Russian Federation. Signed on 16/08/2011.

their foreign counterparts and other competent foreign bodies or persons (FSA Act, §6(2), §18 (3)13).

659. ***Criterion 40.4 –*** For EU Member States and States associated with the Schengen agreement, the police authorities provide feedback to the requested competent authorities in a timely manner upon request, in compliance with the ongoing investigation. This is not a regular approach towards the non-EU Member States. Requirement on provision of feedback is imbedded in several MoUs. Then requested the FIU has the power to send feedback on its initiative or upon request to EU and non-EU counterparts (MLTFPA, §63 (2)). Feedback to foreign counterparts is also provided in compliance with the Egmont Principles.

660. ***Criterion 40.5 –*** In Estonia, there are no unreasonable or unduly restrictive conditions placed on exchanges of information.

661. a) Estonia does not refuse to engage in cooperation with EU Member States on the grounds of fiscal matters is prohibited (CCP, §436(1^2)). The same approach applied also to non-EU Member States.

662. b) The credit institutions and other OEs are required to provide to LEAs requested information, including constituting secrecy swiftly (CIA, §88(5)). There are no financial secrecy laws inhibiting the implementation of AML/CFT measures in the Estonia (see R.9).

663. c) Refusal of a request on the grounds of an ongoing inquiry, investigation, or proceeding is not one of the grounds for prohibition on international cooperation in criminal proceedings unless there are parallel proceedings of the same persons or circumstances (CCP, sections 436, 436^1). However, the execution of the request may be postponed if the assistance would impede national inquiry, investigation, or proceeding. The postponement will be communicated with the requesting country (CCP §436^3 (4)). Disclosure of information concerning pre-trial proceedings is permitted by the Prosecutors Office in the interests of criminal proceedings, of the public, of the data subject as long as it does not induce crime or prejudice the detection of a criminal offence (CCP, §214).

664. d) As a general rule, Estonia does not refuse a request solely on the grounds of the nature of the requesting counterpart authority. The MoJ assesses the formalities of the request, including whether all the necessary details have been provided, the request has been sent by proper authority and translations have been provided. The substantial assessment and decision is made by Prosecutors' Office or court depending on the competences (CCP, §489^8). The disclosure of information is permitted in the interests of criminal proceedings, of the public, of the data subject as long as it does not induce crime or prejudice the detection of a criminal offence. (CCP, §214). There are no unduly restrictions as regards for the FIU and the EFSA (MLTFPA, §53, §63, FSA Act, §6(2), §18(3)13)).

665. ***Criterion 40.6 –*** It is the responsibility of the Prosecutors office to ensure that the provided information is handled correctly (CCP, §214).

666. The information exchanged via Interpol and Europol channels follows the international procedure and handling codes. Only dedicated and authorised personnel in the Prosecutors Office and within the Police have access to the international co-operation channels.

667. The ISS is currently implementing rules for storing and sharing information to comply with national and international regulations. The ISS allows employees to access the information available in the institution according to their professional needs and need for knowledge. The processing of data complies with the relevant laws and procedures concerning the handling of

state secrets and foreign information and information intended for internal use. Internal regulations ensure the lawful use of data. The DPI co-operates with the authority for the lawful use and storage of data and databases. The Security Authorities Surveillance Committee of Riigikogu exercises supervision over the ISS (Security Authorities Act, §36).

668. Only officials of the FIU have access to the information processed within the FIU and the FIU has the right to establish restrictions on forwarded information (MLTFPA, §60(1), §60(8). When registering incoming requests, the information whether the data can be shared and with which authorities, as well as the information to which usage (e.g., intelligence, evidence) is highlighted in the information system of the FIU.

669. According to §47(3) of the FSA Act, the EFSA are entitled to use the rights, powers and in order to fulfil the request of the European supervisory authority, Contracting State and other FSA for the receipt of information, restriction of a right or performance of another act or activity. If the transmitted information is related to ML and TF or the prevention of such activities originates from the competent authority of another Contracting State, the information may be transmitted only with the permission of this authority or within the boundaries established upon grant of such permission.

670. ***Criterion 40.7*** **–** Requests and information from international counterparts are handled confidentially, and the information is only disclosed on a need-to-know basis. The gathered information is only used for the requested purpose and is conveyed through 24/7 or SIENA channels.

671. Disclosure of information is only permitted by the Prosecutors office in the interest of criminal proceedings, the public, or the data subject as long as it does not induce crime or prejudice the detection of a criminal offence, damages the interests of Estonia or the criminal matter, endanger a business secret or violate the activities of a legal person or violate the rights of the data subject or third parties (CCP, §214).

672. A request for information may be refused if it is obvious that a non-EU member state does not ensure an adequate level of data protection. The MoJ decides co-ordination with the Ministry of Foreign Affairs, the DPI, and the Office of the Prosecutor General (CCP, §436(3)).

673. The FIU may refuse to exchange information in cases where the exchange of information is outside the aims of AML/CFT or non-consistent with the FIU and it´s counterparts obligations concerning privacy and data protection. (MLTFPA §63 (2), §63 (7)).

674. The EFSA is obliged to maintain the confidentiality of information they receive in performing their duties as Supervision Authority. Furthermore, the information received are only to be used in the area of prevention, regulation and supervision (FSA Act §34(1), §54 (2), §479(3)). Additionally, the EFSA are only allowed to communicate confidential information with its counterparts if the counterpart can maintain the confidentiality of the information and it is necessary for the counterpart's supervision (FSA Act §54(41).

675. ***Criterion 40.8*** **–** Competent authorities may spontaneously communicate relevant and necessary information in purpose to detect, prevent or investigate criminal offences with imprisonment of at least three years, as specified in the CCP, (§489[6] (1)), e.g., acts of terrorism and ML offences. The Prosecutors office can share information without an MLA as long as the information gathered during an investigation is already in possession. The information can be shared spontaneously or upon request if the prosecutor in charge of the investigation finds it relevant and necessary (CCP §214). The PBGB, can make inquiries solely based on international

police co-operation. The PBGB are allowed to conduct inquiries within a broad range of information and exchange information on criminal proceedings based on EU framework and international agreements.[302] The ISS can conduct inquiries within their international counterparts. The EFSA is entitled to use the rights, powers and information granted to it in order to fulfil the request of the European supervisory authority, Contracting State and its counterparts for the receipt of information, restriction of a right or performance of another act or activity (FSA Act, §47(3)). If the transmitted information is related to ML and TF or the prevention of such activities originates from the competent authority of another Contracting State, the information may be transmitted only with the permission of this authority or within the boundaries established upon grant of such permission.

676. ***Criterion 40.9*** **–** The FIU is an independent authority under the MoF. The legal base for information exchange and international co-operation is stated in section 63 of the MLTFPA. The FIU has the right to exchange information and conclude co-operation agreements with a foreign authority that performs the duties of a financial intelligence unit or a foreign law enforcement or supervisory agency, and an international organisation or institution.

677. ***Criterion 40.10*** **–** The FIU can provide feedback to its international counterparts (MLTFPA s. 63 (2). Since 2020, the FIU has introduced annual feedback collection from its most significant counterparts, including spontaneous forwarding of information. If the provided information has been of especially value, the FIU give spontaneous feedback. Furthermore, the FIU provides feedback when they ask for additional information or request permission to disseminate provided information to other LEAs.[303]

678. ***Criterion 40.11*** **–** The EFIU has the right, both on its initiative and upon request to send and receive any information relating to natural or legal persons in AML and CFT matters (MLTFPA §63(2). The FIU may, if necessary, place restrictions and conditions on the use of information MLTFPA §63(6). The FIU only refuses the exchange of information in exceptional cases and when the information is clearly outside the aims of AML/CFT (MLTFPA, §63 (7, 7^1, 9-10). The provisions of MLTFPA (§, 63) entitles the EFIU to exchange information based on the principle of reciprocity.

679. ***Criterion 40.12*** – The EFSA have the legal basis and general principles for co-operation between the EFSA and its counterparts are stated in Chapter 5 of the FSA Act. There are two permanent mechanisms for international co-operation and information exchange, through supervisory colleges and under bilateral agreements and MOUs. There are also mechanisms for ad-hoc co-operation. The EFSA has a reinforced co-operation with Scandinavia and the Baltics since they are home countries to the leading banking groups in Estonia. The EFSA also have a number of MOUs with EU Member States as well as non-EU states, even though some of them were replaced with the EU legislative framework.[304]

680. The EFSA co-operation is also regulated in chapter 10 of the EFSA AML rules of procedure. Chapter 11 of the guidelines are based on the EBA Joint guidelines on co-operation and

[302] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
[303] 2020-2021 FIU annual overview of international cooperation.
[304] The list of MOU:s is available on https://www.fi.ee/et/finantsinspektsioon/rahvusvaheline-koostoo/koostookokkulepped.

information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions to which Estonia has complied with.[305]

681. No information in available about the legislative framework of cooperation of the EFIU in the capacity of a supervisor.

682. ***Criterion 40.13 –*** The general principles for international cooperation for the EFSA are covered by the provisions of chapter 5 of the FSAA. According to article 54(2), information obtained during financial supervision shall be confidential. The EFSA has the right to exchange confidential information to a foreign FSA only if the receiver is obliged to maintain confidentiality, and the information is necessary for exercising financial supervision. However, according to article 54 (7) of the FSAA, the EFSA has the right to send confidential information essential for the performance of its functions to the subjects of co-operation according to articles 46-47 of the FSAA. Chapter 10 of the EFSA AML rules of procedure, provides the principles of co-operation as home or host supervisor, including taking simultaneous and coordinated supervisory actions with relevant FSAs of other countries.

683. No information in available about the legislative framework of cooperation of the EFIU in the capacity of a supervisor.

684. ***Criterion 40.14 –*** The ground principles for cooperation with foreign supervisors is covered by the provisions of chapter 5 of the FSAA and chapter 10-11 of the EFSA AML rules of procedure. Within the EU, the EFSA can exchange any information that a competent authority in another state within the EEA requires for its supervision, which means that regulatory, prudential, and AML/CFT information can be provided (FSAA, Art.46-50).

685. No information in available about the legislative framework of cooperation of the EFIU in the capacity of a supervisor.

686. ***Criterion 40.15 –*** The EFSA is entitled to use the rights, powers and information granted to it by the FSAA and other legislation or on the basis thereof to fulfil the request of the European Supervisory authority, Contracting State and other foreign financial supervision authority for the receipt of information, restriction of a right or performance of another act or activity (FSAA, §47 (3).

687. No information in available about the legislative framework of cooperation of the EFIU in the capacity of a supervisor.

688. ***Criterion 40.16*** – The information provided from counterparts to the EFSA may be transmitted only with authorisation from the providing authority or within the boundaries established upon grant of such permission (FSAA, §47 (3)). The EFSA has the right to permit its counterparts to disclose confidential information on the grounds of article 54 of the FSAA. Information received from counterparts may be disclosed if a respective agreement has been entered with the foreign counterpart. The entered MOUs includes provisions on data protection and privacy rules.

---

[305] https://www.eba.europa.eu/sites/default/documents/files/document_library//Joint%20Guidelines%20on%20cooperation%20and%20information%20exchange%20on%20AML%20-%20CFT.pdf, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2018/EBA-CP-2018-11-08%20CP%20on%20ESAs%20on%20guidelines%20on%20cooperation%20and%20information%20exchange/Final%20guidelines/936145/JC%20GL%202019%2081%20-%20JC%20GLs%20on%20cooperation%20and%20information%20exchange_100620.pdf

689. No information in available about the legislative framework of cooperation of the EFIU in the capacity of a supervisor.

690. ***Criterion 40.17 –*** The legal base described for under c.40.2 provides also the legal ground for LEAs international cooperation. LEAs can exchange domestically available information with foreign counterparts for intelligence as well as for investigation purposes. This includes ML, TF offences as well as predicate offences (Council Framework Decision 2006/960/JHA of 18 December on simplifying information exchange and intelligence, CCP, ss 508.[78], 508.[81-84]). The ARO can exchange information with its counterparts governed by the Council Decision 2007/845/JHA.

691. Outside of the criminal investigation based of the internal legislation of the European Union, especially within Customs Network cooperation (LEWP etc), ETCB uses Naples II Convention (customs) or Council Framework Decision 2006/960/JHA of 18 December 2006 2006/960/JHA (taxes) to share information for intelligence purposes.

692. ***Criterion 40.18*** – The general principles for international cooperation in CCP, section 433 is applicable on the PBGB and ISS information exchange with their counterparts as part of the INTERPOL, EUROPOL and EUROJUST as well as multi- and bilateral agreements and the legislative framework within the EU. This includes to conduct inquiries and obtain information, e.g., in databases accessible for domestic LEAs and covert operations (CCP, §433, §489.[2,] §489.[6], §489.[43-45], §489.[54)]. The cooperation with non-EU counterparts is based on the provision of multi- and bilateral agreements. The PBGB has 10 intergovernmental agreements and 7 interinstitutional cooperation plans.[306]

693. ***Criterion 40.19*** – Estonia is able to set up joint investigative teams. The establishment of a joint investigation team is decided by the Office of the Prosecutor´s General and the JIT is headed by the Prosecutor's Office. JITs can be concluded with EU Member States and third countries (CCP s. 471, EU Conventions and multi- or bilateral agreements).

694. ***Criterion 40.20 –*** A Cooperation Agreement between the PBGB, the Prosecutor's Office and the FSA regulates the activities of the parties cooperation, exchange of information and training to prevent the exploitation of the financial sector for criminal purposes and to prevent, deter, detect and prosecute offences involving securities and subjects of public financial supervision. Clause 17 of the Annex provides that the parties are to cooperate in international relations in so far as they relate to the competence of the other party. The form and extent of cooperation shall be decided by the party directly involved in international relations (Postipoiss system ref. 29 September 2009 PA 3.4-1.5/5)).

695. The PBGB relies as legal basis on the conditions set out in Council Decision 2007/845/JHA[307] on establishing and cooperation between ARO and Council Decision 2006/960/JHA[308] on simplifying information exchange. The PBGB doesn´t refuse a request for assistance because the nature or status of the requesting counterpart authority is different from

---

[306] Latvia, Finland, Hungary, Moldova, Belgium, Cyprus, Slovenia, United Kingdom and Germany. There are interinstitutional cooperation plans with the Finnish National Police Board, Helsinki Police Department, South-Eastern Finland Police Department, Latvian and Lithuanian Public Order Police Units, Riga Region Police Department, State of Rhineland-Palatinate and with the Federal Security Service of the Russian Federation.

[307] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime

[308] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

that of its foreign counterpart. It will be decided case by case, and all relevant circumstances will be considered, e.g., GDPR[309], preventable damage etc.

696. The FIU has the right to exchange information with a foreign law enforcement or supervisory agency, as well as an international organisation or institution. The FIU cannot exchange the information that is obtained by fulfilling the primary role of the FIU for the purposes of supervision. However, The FIU can exchange information with foreign counterparts if the FIU has obtained the information in supervisory proceedings and the proceedings are not ongoing (MLTFPA § 63).

697. The FSA can use the rights, powers and information granted to it by the FSA Act and other legislation or on the basis thereof in order to fulfil the request of the European supervisory authority, Contracting State and other foreign financial supervision authority for the receipt of information. (FSAA §47(3), §54(4^1).

698. Both LEA-s and Prosecutor's Office can share information which is considered relevant for another authority or another country. In case information has been obtained during the criminal investigation, Section 214 of the CCP applies and decision on the information disclosure and its scope is done by the Prosecutor's Office. For international cooperation purposes CCP Section 473 (Spontaneous exchange of information) and Section 508.84 (Spontaneous exchange of information between EU Member States) can be used and information shared with competent authority of a foreign state.

Weighting and Conclusion

699. Competent authorities have the powers to provide a wide range of international assistance. There was no supporting information made available to confirm the EFIU powers for international cooperation in its role of a supervisor. **R.40 is rated LC.**

[309] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Summary of Technical Compliance – Deficiencies

ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk–based approach	**PC**	• There are significant shortcomings with the application of the country-wide risk assessment methodology and the outcomes of the assessment; other strategic analyses need to be further developed in order to fill the gaps in the understanding of risk (c.1.1) • Nation-wide policies to guide risk-based decisions have not been available for the whole period under consideration and are not reflected in strategies and work-plans of the competent authorities (c.1.5) • Exceptions from the AML/CFT framework are not supported by substantive assessment of ML/TF risks (c.1.6)
2. National co–operation and coordination	**C**	
3. Money laundering offences	**LC**	• There is gap in the range of predicate offence related to TF. • Sanctions for ML offence for natural persons are not fully dissuasive.
4. Confiscation and provisional measures	**C**	
5. Terrorist financing offence	**LC**	• Definition of TF offence does not meet all criteria required under R.5, since financing of the offences listed in the Annex of the TF Convention is not considered to be a TF offence.
6. Targeted financial sanctions related to terrorism & TF	**PC**	• The Guidelines do not specify that the authorities will follow the procedures established by the UN Committees when prospering designations. (6.1) • The legislation does not stipulate that Estonia shall specify whether its status as a designating state may be made known. (6.1) • At the national level, there is no formalised procedure under which Estonia would request another country to give effect to freezing measures undertaken by competent authorities. (6.2) • Requirement to freeze assets is to be applied in the certain circumstances only, which limits the compliant application of those. (6.5) • The scope of assets that should be considered when implementing freezing obligations is limited. (6.5) • Prohibition to make available funds and other assets are limited only to designated persons and to listed activities. (6.5) • The EFIU and EFSA Guidelines together do not specifically target all FIs and DNFBPs as required by the FATF Standard. • There are no provisions adopted to protect the rights of *bona fide* third parties acting in good faith when implementing the international financial sanctions. • There are various mechanisms for reconsideration of the designations but none of them explicitly provide competent authority and the process.
7. Targeted financial sanctions related to proliferation	**PC**	• Requirement to freeze assets is to be applied in the certain circumstances only, which limits the compliant application of those. • The scope of assets that should be considered when implementing freezing obligations is limited. • Prohibition to make available funds and other assets are limited only to designated persons and to listed activities. • The EFIU and EFSA Guidelines together do not specifically target all FIs and DNFBPs as required by the FATF Standard. • There are no provisions adopted to protect the rights of bona fide third parties acting in good faith when implementing the international financial sanctions. • There are various mechanisms for reconsideration of the designations but none of them explicitly provide competent authority and the process. • There are various sanctions set forth for the failure to comply with obligations under R.7, but gaps exist • There is no provision 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.

8. Non–profit organisations	**PC**	• Major improvements are required to enhance the knowledge about the TF vulnerabilities in the sector, including identification of the specific subset of the NPOs. • Estonia did not identify the nature of the threats posed by terrorist entities to the NPOs which are at risk, as well as how these can be abused. • Estonia has not reviewed the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for TF support. • Estonia did not yet implement measures for encouraging the NPOs to conduct their transactions through formal financial channels. • Estonia did not demonstrate yet should taking steps to promote effective supervision or monitoring such that they are able to demonstrate that risk-based measures apply to NPOs at risk of terrorist financing abuse. • The monitoring and supervising in place does not address the requirements of R.8 and apply risk – based sanctions to target NPOs.
9. Financial institution secrecy laws	**C**	
10. Customer due diligence	**LC**	• The MLTFPA does not provide for the obligation to verify the BO's identity based on information and data obtained from a reliable source. (10.5) • There is no express obligation to obtain information on the legal form of the legal person. (10.9) • There is no obligation to obtain the information on the registered office/ place of business during the identification process of a legal entity. (10.9) • The standard requires that the measures for identifying the ultimate controlling interest, via ownership and other type of control, to have a "cascading" systematic process, the obligation under §9(1)1)) appears instead to offer two *alternative* options. (10.10) • The MLTFPA does not include the beneficiary of the life insurance policy among the factors characterising a higher risk (described under §36(2), §37), except for the cases when the beneficiary of the life insurance policy or the BO of the beneficiary is a PEP. (10.13) • There is no explicit requirement that FIs should adopt risk management procedures concerning the exceptions described under c.10.14 (10.15) • Amendments of the MLTFPA (about nine during the period of 2018-2021) appear not to impose the obligation for the obliged entities to re-apply the new CDD requirements to the existing customers over a period of one year from the entry into force – this obligation had been present in previous amendments to the MLTFPA. (10.16) • There is no express legal provision to permit the FIs not to complete CDD in cases where there is a ML/TF suspicion and reasonable belief that performing the CDD process would tip-off the customer. (10.20)
11. Record keeping	**C**	
12. Politically exposed persons	**LC**	• Siblings are not covered as family members of a PEP. (12.3) • The indicators for suspicions do not include life insurance policies that have been identified as PEPs. (12.4)
13. Correspondent banking	**PC**	• For correspondent relationships within the EEA, a risk-based approach is taken, however R13 requires that the application of the measures established under 13.1 must apply to <u>all</u> cross-border correspondent banking relationships. (13.1) • Payable through account requirements apply to respondent institutions outside the EEA and only on a risk basis to those within the EEA. (13.2)
14. Money or value transfer services	**LC**	• In Estonia there is no specifically designated authority for detecting unlicensed MVTS activities. (14.2) • There is no explicit requirement to include the agents of a principal in that principal's AML/CFT programmes and monitor them for compliance with these programmes. (14.5)

15. New technologies	**PC**	• New Technology risk assessments are not always accompanied with in-depth analysis. (15.1) • There is no explicit requirement to undertake a risk assessment prior to the launch or use of such products, practices and technologies. (15.2) • The NRA acknowledged that the available quantitative and qualitative data did not allow for the establishing of patterns, the profile of criminals or suspicious activities related to VASPs in Estonia. (15.3) • In Estonia there is no specifically designated authority for detecting unlicensed VASP activities. (15.5) • It is not clear how the RBA models of the EFSA and the EFIU take into account the degree of discretion allowed to the covered FIs under the risk-based approach. (15.6) • There is, need for further guidance of sector specific typologies, in particular in respect to TF. This is especially important considering the materiality of the sector and a high level of TF risks in the sector. (15.7) • The sanctions available for FIs apply equally to VASPs including the shortcomings under c.35.1 (15.8) • There is no express requirement to obtain and hold the information regarding the name of the beneficiary. (15.9) • There is no express requirement for the originator and beneficiary VASPs to make available information, on request, to appropriate authorities. (15.9) • There is no requirement for the beneficiary VASP to perform post-event or real time monitoring in case of transfers which lack required originator or beneficiary information. Likewise, the beneficiary VASPs are not required to have risk-based policies and procedures in order to determine whether to reject or suspend a VA transfer and take appropriate follow-up up actions. (15.9) • There are no legal provisions to ensure that the same obligations apply to FIs when sending or receiving virtual assets transfers on behalf of a customer. (15.9) • There are no guidelines provided to VASPs on their obligation to take action under the freezing mechanism. The sanctions applicable to VASPs for non-compliance with the obligations under R.7 are identical to the ones that apply to covered FIs and the deficiencies as per c.7.3, especially concerning the lack of sanctions for non-compliance with the freezing obligation. (15.10) • The deficiency with respect to issues on double-criminality requirement apply (see c.37.6). (15.11)
16. Wire transfers	**C**	
17. Reliance on third parties	**LC**	• The list of CDD measures under §20(1) that can be performed by other persons includes the "the monitoring of a business relationship", which falls out of the FATF standard. (17.1) • The MLTFPA does not define the term "*another person*" that can be relied upon. From the provisions of §24(3) it appears that the "*other person*" who is relied on is required to comply and actually does comply with requirements equal to those established by the Directive (EU) 2015/849. Thus, this does not appear to be consistent with the definition of "third party" in the FATF Standards which is limited to FIs and DNFBPs that are "regulated, supervised and monitored". (17.1) • FIs are not allowed to rely on third parties established in high-risk third countries (MLTFPA, §24(6)). This is limited to jurisdictions outside the EU/EEA area, as listed by the Regulation (EU) 2016/1674 and does not fully satisfy the requirement to regard the information on the level of country risk. (17.2) • When part of the same group, covered FIs are permitted to rely only on persons established in a country (both EU and non-EU) where requirements equal to those of EU AML/CFT Directive apply. However, these requirements are not established by the MLTFPA, which provides for ML/TF risk mitigating measures only in relation to high risk third countries (outside EAA). (17.3)

18. Internal controls and foreign branches and subsidiaries	**LC**	• The sectoral legislation requires FIs supervised by the EFSA and EFIU, except for the investment firms, to have an independent audit function. (18.1) • Covered FIs are required to ensure that their foreign branches and majority-owned subsidiaries comply with the requirements established under the MLTFPA. This does not apply to cases when the host country is an EU members state. (18.3)
19. Higher–risk countries	**PC**	• FIs are required to apply the EDD measures towards countries listed by the EU, which is narrower than the FATF approach. • No legal basis is provided for the application of countermeasures by Estonia either when called for by the FATF or independently. • Sufficient measures to ensure FIs are advised about the countries with weak AML/CFT systems are in place only for FIs supervised by the EFSA.
20. Reporting of suspicious transaction	**PC**	• The MLTFPA does not explicitly provide that FIs should submit a report when they have reasonable grounds to suspect that funds are the proceeds of crime or are TF-related. • Deficiencies in criminalisation of TF restrict the scope of the TF reporting requirement (see R.5).
21. Tipping–off and confidentiality	**PC**	• FIs may inform interested persons that the EFIU has restricted the use of their account after the FI has complied with the FIU's compliance notice, essentially tipping off the interested persons.
22. DNFBPs: Customer due diligence	**LC**	• CDD Measures under R10 apply to DNFBPs. Deficiencies that apply to FI's identified in R.10 apply to DNFBPs. (22.1) • See R.12 for a detailed description of measures taken by Estonia to comply with the PEPs requirements and the identified gaps. (22.3) • See R.15 for a detailed description of measures taken by Estonia to comply with the new technologies requirements and the identified gaps. (22.4) • See R.17 for a detailed description of measures taken by Estonia to comply with the reliance on 3rd parties requirements and the identified gaps. (22.5)
23. DNFBPs: Other measures	**PC**	• DNFBPs, are required to report suspicious transactions based on the same provisions of the MLTFPA as FIs. Dealers involved in the purchase and sale of precious metals used or production, scientific or medical purposes are not obliged entities and so they are not subject to the obligation to report. (23.1) • Requirements described in relation to FIs under R.18.1 are equally applicable to DNFBPs. (23.2) • Requirements and shortcomings described in relation to FIs under R.19 are equally applicable to DNFBPs. (23.3) • Requirements and shortcomings described in relation to FIs under R.21 are equally applicable to DNFBPs. (23.4)
24. Transparency and beneficial ownership of legal persons	**PC**	• Available analyses do not appear to provide a reliable assessment of the ML/TF risks associated with all types of legal persons created in the country (c.24.2) • The regulations in place do not provide for a number of elements of the FATF requirements for maintaining basic information (c.23.4) • There are insufficient mechanisms to ensure that basic information is accurate and updated on a timely basis (c.24.5) • There are insufficient measures to ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner (c.24.8) • Information made available to the assessment team does not enable a conclusion that the companies are required to maintain the information and records referred to for at least 5 years (c.24.9)
25. Transparency and beneficial ownership of legal arrangements	**PC**	• There is no effective requirement for trustees to maintain the information specified under c.25.1(a), as well as to obtain and maintain information specified under c.25.1(b) (c.25.1(c)) • There are no sufficient measures in place to ensure that trustees disclose their status to financial institutions and DNFBPs (c.25.3)

		• The arrangements in place would effectively prevent trustees from providing relevant information to competent authorities, financial institutions and DNFBPs (c.25.4) • Liability for the failure of trustees to comply with relevant obligations is partially enforceable (c.25.7) • No sanctions are available for the failure of trustees to otherwise grant to competent authorities' timely access to information held by them (c.25.8)
26. Regulation and supervision of financial institutions	**LC**	• Companies managing a mandatory pension fund and life insurance companies providing services related to mandatory funded pension insurance contracts are excluded from the scope of AML/CFT supervision. There is no formal assessment (in the NRA or other documents) that would justify these exemptions. (26.1) • The assessment of the country's compliance with the IOSCO Principles was carried out prior to becoming a signatory to the IOSCO MMOU in 2011. The assessment of Estonia against the Insurance Core Principles (ICP) of the IAIS was carried out in 2000 as part of the Financial Sector Assessment Programme (FSAP) and in 2011 when Estonia applied for OECD Membership. (26.4) • Given the significant time since the last external evaluations, their conclusions are no longer considered to be relevant. • It is not clear how the RBA models of the EFSA and the EFIU take into account the degree of discretion allowed to the covered FIs under the risk-based approach. (26.5) • The Code of conduct for the supervision activities of the EFIU does not provide for periodical reviews. (26.6)
27. Powers of supervisors	**LC**	• The shortcomings identified under R.35 apply (see R.35) (27.4)
28. Regulation and supervision of DNFBPs	**PC**	• DPMSs which are carrying out certain activities (see R.1.6) are excluded from the AML/CFT obligations and, therefore, not subject to monitoring compliance with AML/CFT requirements. (28.3) • The provisions for refusal of registration by the MoJ (for Notaries), BA and the Auditor Oversight Board do to not cover association with criminals. Real estate agents, accountants and tax consultants are not subject to any professional accreditation. (28.4) • It is not clear how the RBA models of the EFIU take into account the degree of discretion allowed to the covered DNFBPs under the risk-based approach. (28.5) • The BA does not undertake a risk-based supervision regime, but rather is caring out its inspections applying a random sample. (28.5) • Inspection of Notaries is not risk-based however, the planned supervisory activities of CN, pursuant to the annual inspection plans, must take into account some risk-related elements. (28.5)
29. Financial intelligence units	**LC**	• This MLTFPA limits the mandate of the EFIU, not also extending it to ML predicate offences, and dissemination of results of its analysis. While the legislation defined STRs in a wider manner, referring to ML, TF and related offences, the duties of the FIU are defined in a narrower manner as dealing with "information referring to ML and TF". • The legislation is precise on dissemination of information held with the FIU, but it is not clear on dissemination of the results of the FIU analysis to authorities other than the supervisory authority.
30. Responsibilities of law enforcement and investigative authorities	**C**	
31. Powers of law enforcement and investigative authorities	**C**	
32. Cash couriers	**LC**	• There is no declaration system in place for persons leaving to/entering from another EU Member State. • There is no EU-internal border declaration system for cash or BNIs through mail or cargo.

33. Statistics	**PC**	• Estonian authorities do not maintain comprehensive statistics on ML/TF investigations, prosecution, and conviction as well as data on seizure and confiscation.
34. Guidance and feedback	**LC**	• No guidance is provided on TF-specific typologies and schemes, especially to the sectors with higher risk exposure
35. Sanctions	**PC**	• In the case of PSPs, EMIs and credit providers, the powers are significantly more limited compared to those of the EFIU in relation to the FIs under its supervision and, therefore, cannot be considered as having an effective, proportionate or dissuasive character. (35.1) • The financial penalty under misdemeanour proceedings does not feature the characteristics of an effective, proportionate and dissuasive sanction. (35.1) • In relation to TFS obligations, the sanctions under the misdemeanour proceedings do not extent to all OEs and do not cover the compliance with obligation to freeze without delay and prior notification. (35.1) • No sanctions are available for the NPOs for the non-compliance with the requirements of R.8. (35.1)
36. International instruments	**LC**	• Estonia did not fully implement the International Convention for the Suppression of the Financing of Terrorism.
37. Mutual legal assistance	**LC**	• Principal of dual criminality applied in Estonia can limit the ability to provide MLA for TF offence.
38. Mutual legal assistance: freezing and confiscation	**LC**	• There is no legal basis for providing assistance to non-EU member states if the request is related to non-conviction-based confiscation.
39. Extradition	**LC**	• Deficiencies identified in incrimination of the TF offence may limit the execution of the extradition of the foreign request since dual criminality is required.
40. Other forms of international co–operation	**LC**	• There was no supporting information made available to confirm the EFIU powers for international cooperation in its role of a supervisor.

GLOSSARY OF ACRONYMS[310]

	DEFINITION
BA	Bar Association of Estonia
BR	Business Register
BOE	Bank of Estonia (Eesti Pank)
BOID	Beneficial Ownership Information Database
CCP	Code of Criminal Procedure
CI	Credit institution
CN	Chamber of Notaries of Estonia
COC	Commercial Code
CR	Commercial Register
DNFBP	Designated non-financial business or profession
DPI	Data Protection Inspectorate
EBA	European Banking Authority
ECB	European Central Bank
ECRS	Estonian Central Register of Securities
EFIU	Estonian Financial Intelligence Unit
EFSA	Estonian Financial Supervision Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
ETCB	Estonian Tax and Customs Board
FA	Foundations Act
FI	Financial institution
GPCCA	General Part of the Civil Code Act
ISS	Internal Security Service
MEQ	Mutual Evaluation Questionnaire
MLTFPA	Money Laundering and Terrorist Financing Prevention Act
MEAC	Ministry of Economic Affairs and Communications
MFA	Ministry of Foreign Affairs
MoJ	Ministry of Justice
NCP	National Criminal Police
NPAA	Non-Profit Associations Act
NPAR	Register of Non-Profit Associations and Foundations
NRA	National risk assessment
OE	Obliged entity
PBGB	Police and Border Guard Board
PO	Prosecutor's Office
RBA	Risk-based approach
SRB	Self-regulatory body
SGC	Strategic Goods Commission of the Ministry of Foreign Affairs

[310] Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

www.coe.int/MONEYVAL

December 2022

Anti-money laundering and counter-terrorism financing measures

Estonia

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Estonia as at the date of the on-site visit (25 April - 6 May 2022). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Estonia's AML/CFT system