COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM (MONEYVAL)

MONEYVAL(2014)20

# Report on Fourth Assessment Visit

## Anti-Money Laundering and Combating the Financing of Terrorism

# ESTONIA

18 September 2014

Estonia is a member of MONEYVAL. This evaluation was conducted by MONEYVAL and the mutual evaluation report on the 4th assessment visit of Estonia was adopted at its 45th Plenary (Strasbourg, 15 – 19 September 2014).

# TABLE OF CONTENTS

## LIST OF ACRONYMS USED

| | |
|---|---|
| AML/CFT | Anti-money laundering/combating the financing of terrorism |
| ARB | Asset Recovery Bureau |
| CDD | Customer Due Diligence |
| CETS | Council of Europe Treaty Series |
| CC/PC | Penal Code |
| CCP | Code of Criminal Procedure |
| CoE | Council of Europe |
| CrIA | Credit Institutions Act |
| CTRs | Cash Transaction Reports |
| DNFBPs | Designated Non-Financial Businesses and Professions |
| ECSD | Estonian Central Securities Depository |
| EEA | European Economic Area |
| ETS | European Treaty Series [since 1.1.2004: CETS = Council of Europe Treaty Series] |
| ETCB | Estonian Tax and Customs Board |
| EU | European Union |
| EUR | Euros |
| FATF | Financial Action Task Force |
| FI | Financial institution |
| FIU | Financial Intelligence Unit |
| FSA | Financial Supervision Authority |
| FT/TF | Financing of terrorism |
| ISA | International Sanctions Act |
| ISS | Internal Security Service |
| IT | Information technologies |
| LEA | Law Enforcement Agency |

| | |
|---|---|
| MER | Mutual evaluation report |
| ML | Money laundering |
| MLA | Mutual Legal Assistance |
| MLAT | Mutual Legal Assistance Treaty |
| MLTFPA | Money Laundering and Terrorist Financing Prevention Act |
| MoI | Ministry of Interior |
| MoU | Memorandum of Understanding |
| NCP | National Criminal Police |
| NENO | Network of Estonian Non-profit Organisations |
| NPAA | Non-Profit Associations Act |
| NPO | Non-profit organisation |
| NRA | National Risk Assessment |
| PC | Penal Code |
| PEP | Politically Exposed Person |
| PBGB | Police and Border Guard Board |
| SAR | Suspicious activity report |
| SRO | Self-Regulatory Organisation |
| STR | Suspicious transaction report |
| UN | United Nations |
| (UN)CTED | (United Nations) Counter-Terrorism Executive Directorate |
| UNSCR | United Nations Security Council Resolution |

# I. PREFACE

1. This is the fourth report in MONEYVAL's fourth round of mutual evaluations, following up the recommendations made in the third round. This evaluation follows the current version of the 2004 AML/CFT Methodology, but does not necessarily cover all the 40+9 FATF Recommendations and Special Recommendations. MONEYVAL concluded that the 4th round should be shorter and more focused and primarily follow up the major recommendations made in the 3rd round. The evaluation team, in line with procedural decisions taken by MONEYVAL, have examined the current effectiveness of implementation of all key and core and some other important FATF recommendations (i.e. Recommendations 1, 3, 4, 5, 10, 13, 17, 23, 26, 29, 30, 31, 32, 35, 36 and 40, and SR.I, SR.II, SR.III, SR.IV and SR.V), whatever the rating achieved in the 3rd round.

2. Additionally, the examiners have reassessed the compliance with and effectiveness of implementation of all those other FATF recommendations where the rating was NC or PC in the 3rd round. Furthermore, the report also covers in a separate annex issues related to the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter the "Third EU Directive") and Directive 2006/70/EC (the "implementing Directive"). **No ratings have been assigned to the assessment of these issues.**

3. The evaluation was based on the laws, regulations and other materials supplied by Estonia and information obtained by the evaluation team during its on-site visit to Estonia from 10 to 16 November 2013 and subsequently. During the on-site visit, the evaluation team met with officials and representatives of relevant government agencies and the private sector in Estonia. A list of the bodies met is set out in Annex 1 to the mutual evaluation report.

4. The evaluation was conducted by an assessment team, which consisted of members of the MONEYVAL Secretariat and MONEYVAL experts in criminal law, law enforcement and regulatory issues and comprised: Mr Tomislav Sertic (Assistant Director General, Tax Administration - Central Office, Ministry of Finance, Croatia) who participated as a legal evaluator, Ms Renata Fejes Ujvariné (Economist at the Department of International Finance of the Hungarian Ministry for National Economy, Hungary) and Mr Hamish Armstrong (Senior Manager, Financial Crime Policy at the Jersey Financial Services Commission, United Kingdom Crown Dependency of Jersey) who participated as financial evaluators and Mr Boudewijn Verhelst (Deputy Director of the Belgian CTIF/CFI, Belgium),who participated as a law enforcement evaluator. The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs), as well as examining the capacity, the implementation and the effectiveness of all these systems.

5. The structure of this report broadly follows the structure of MONEYVAL and FATF reports in the 3rd round, and is split into the following sections:

    1. General information
    2. Legal system and related institutional measures
    3. Preventive measures - financial institutions
    4. Preventive measures – designated non-financial businesses and professions
    5. Legal persons and arrangements and non-profit organisations
    6. National and international cooperation
    7. Statistics and resources

Annexes (implementation of EU standards and relevant new laws and regulations)

6. This 4th round report should be read in conjunction with the 3rd round adopted mutual evaluation report (as adopted at MONEYVAL's 28th Plenary meeting – December month 2008), which is published on MONEYVAL's website[1]. FATF Recommendations that have been considered in this report have been assigned a rating. For those ratings that have not been considered the rating from the 3rd round report continues to apply.

7. Where there have been no material changes from the position as described in the 3rd round report, the text of the 3rd round report remains appropriate and information provided in that assessment has not been repeated in this report. This applies firstly to general and background information. It also applies in respect of the 'description and analysis' section discussing individual FATF Recommendations that are being reassessed in this report and the effectiveness of implementation. Again, only new developments and significant changes are covered by this report. The 'recommendations and comments' in respect of individual Recommendations that have been re-assessed in this report are entirely new and reflect the position of the evaluators on the effectiveness of implementation of the particular Recommendation currently, taking into account all relevant information in respect of the essential and additional criteria which was available to this team of examiners.

8. The ratings that have been reassessed in this report reflect the position as at the on-site visit in November 2013 or shortly thereafter.

[1] http://www.coe.int/moneyval

# II. EXECUTIVE SUMMARY

## 1. Background Information

1. This report summarises the major anti-money laundering and counter-terrorist financing measures (AML/CFT) that were in place in Estonia at the time of the 4th on-site visit (10 to 16 November 2013) and immediately thereafter. It describes and analyses these measures and offers recommendations on how to strengthen certain aspects of the system. The MONEYVAL 4th cycle of assessments is a follow-up round, in which Core and Key (and some other important) FATF Recommendations have been re-assessed, as well as all those for which Estonia received non-compliant (NC) or partially compliant (PC) ratings in its 3rd round report. This report is not, therefore, a full assessment against the FATF 40 Recommendations and 9 Special Recommendations but is intended to update readers on major issues in the AML/CFT system of Estonia.

## 2. Key findings

2. **Estonia has taken several important steps to improve compliance with the FATF Recommendations and has registered progress in several areas since the 3rd round evaluation.** Several pieces of legislation were amended and new legislative instruments and guidance were issued to address deficiencies identified in the 3rd round evaluation.

3. **In 2012, Estonia started conducting a national risk assessment, which at the time of the evaluation was still underway**. Institutional risk assessments, which are carried out on a regular basis by the Financial Intelligence Unit (FIU) and the Financial Supervision Authority (FSA), indicate that the highest ML/FT risk derives from business conducted with customers from certain neighbouring countries. Certain financial institutions and DNFBPs, especially payment services (including alternative payment services) and traders in precious metals, are particularly vulnerable to ML/FT. The widespread use of IT in Estonia increases vulnerability to the ML/FT risk within the financial sector. The most common predicate offences are drug trafficking, fraud and tax-related offences. The authorities consider the risk of FT to be low.

4. **The money laundering offence in Estonia is broad, largely covering all the elements of the Vienna and Palermo Conventions.** The authorities have been effective in securing ML convictions for self-laundering, third party laundering and stand-alone ML. Some issues remain within the judiciary regarding the level of proof required to establish the underlying predicate criminality.

5. **The financing of terrorism offence was amended since the third round to address certain deficiencies.** However, further amendments will still be required to ensure that the offence is fully aligned with the Terrorist Financing Convention**.** In particular, the collection of funds to be used by an individual terrorist for any purpose other than terrorist purposes does not appear to be covered. Additionally, not all the acts which constitute an offence under the UN treaties annexed to the TF Convention are fully covered under the FT offence. Since the existing legislative framework has not been tested in practice it is difficult to assess the effectiveness of the system.

6. **The authorities have been effective in confiscating and seizing property in ML and drug-related cases, although the volume of confiscated property seems low in some cases.** The legal framework governing confiscation and provisional measures is still missing certain technical elements, such as confiscation of corresponding value to laundered property and instrumentalities in some cases. The authorities should apply confiscation and seizure measures to other serious proceeds-generating crimes on a more regular basis.

7. **Estonia has implemented the UN Security Council Resolutions mainly through EU legislation.** As a result, the requirement to apply freezing measures without delay is not met. Estonia has not issued a domestic list to apply freezing measures to EU internals and there are still

no clear publicly-known procedures for un-freezing funds and assets in a timely manner. While guidance and communication to the financial and non-financial sector are adequate, supervision is insufficient.

8. **The Estonian FIU is a structurally independent unit within the Police and Border Guard Board and has sufficient human and technical resources to conduct its functions properly.** It has ample powers to request and obtain additional information both from other authorities and reporting entities. Guidance has been provided to reporting entities on the manner of reporting. On the whole, the FIU appears to be functioning effectively and efficiently.

9. **Overall progress has been made to strengthen the preventive AML/CFT system.** The Money Laundering and Terrorist Financing Prevention Act (MLTFPA) introduced the concept of the risk-based approach and includes, inter alia, provisions catering for simplified and enhanced customer due diligence (CDD) measures. CDD, record-keeping and reporting requirements are all broadly in line with the FATF Recommendations. Some weaknesses in the identification of beneficial owners by certain financial institutions were identified. The reporting level by financial institutions appears to be adequate. The legal framework for monitoring complex, unusual large transactions and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations is still deficient.

10. **The AML/CFT supervisory framework is broadly sound, especially with respect to the supervision of financial institutions subject to FSA supervision.** The authorities have used their powers to stop criminals from owning or controlling financial institutions. The FIU, which supervises financial institutions not subject to the Core Principles, needs to be strengthened further. In particular, supervisory staff at the FIU needs to be increased.

11. **The sanctioning regime for AML/CFT breaches needs to be revised as it still does not provide for the whole range of sanctions required under the FATF Recommendations**. In practice, the sanctions imposed by the FSA and the FIU are very low.

12. **The preventive measures applicable to DNFBPs are largely in place.** Overall, DNFBPs appear to be aware of their obligations. However, implementation of preventive measures varies across the sector. The weakest element in the system, insofar as awareness of preventive measures is concerned, appears to be real estate intermediaries. It is encouraging that Estonian attorneys seem to take their reporting obligation more seriously than in most countries. Supervision of DNFBPs needs to be improved, especially in terms of the number of on-site visits conducted and sanctions imposed.

13. **Cooperation and coordination between competent authorities on a domestic level appears to be conducted in an effective manner.** The government committee set up for the purpose of coordination of AML/CFT policies in Estonia has produced tangible results.

14. **The Estonian mutual legal assistance framework allows the judicial authorities to give sufficient assistance in money laundering and terrorism financing cases.** The legal provisions regulating the mutual legal assistance appear to be effectively applied in practice by Estonian authorities. The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect of the scope of the TF offence.

15. **No significant progress has been made in order to address the deficiencies relating to the transparency of legal persons identified in the 3rd round assessment.** Accessibility to company information online has however been greatly improved.

16. **The Estonian authorities have significantly improved the legal framework regulating non-profit organisations (NPOs).** As a result of an assessment carried out by the FIU, NPOs were included under the scope of the MLTFPA and are now subject to preventive measures.

## 3. Legal Systems and Related Institutional Measures

17. The money laundering offence is broadly in line with the Vienna and Palermo Conventions. Since the 3rd round, Estonia introduced the concept of conspiracy within its Penal Code to ensure that all ancillary offences to ML are covered. The authorities have been effective in securing ML convictions for self-laundering, third party laundering and stand-alone ML. Although the ML offence does not specifically require a simultaneous or prior conviction for the predicate offence, some issues remain within the judiciary with respect to the level of proof required to establish the underlying predicate offence. The authorities should therefore continue training prosecutors and judges on evidential thresholds for establishing underlying predicate criminality and confront the judiciary with more cases where it is not possible to establish precisely the underlying offence(s).

18. The financing of terrorism offence has been amended to address some deficiencies identified in the 3rd round evaluation. However, the offence is still not entirely aligned with the Terrorist Financing Convention. In particular, the collection of funds to be used, in full or in part, by an individual terrorist for any purpose other than terrorist purposes is still not covered. Not all the acts which constitute an offence under the UN treaties annexed to the TF Convention are fully covered under the FT offence. Those acts which are covered under the FT offence are subject to an additional purposive element which goes beyond the FT convention. In view of the deficiencies in the FT offence it is doubtful whether criminal proceedings could be initiated in Estonia where a person finances a terrorist act committed abroad.

19. Confiscation and seizure of property in ML and drug-related offences appear to be regularly utilised, although to a lesser extent for other serious proceeds-generating crimes. The volume of confiscated property appears to be on the lower end of the scale. Legislation on confiscation and provisional measures has remained unchanged since the 3rd round evaluation. While the Penal Code broadly provides for a confiscation mechanism to deprive criminals of their ill-gotten gains, some technical deficiencies still need to be addressed. Confiscation of property of corresponding value to laundered property and instrumentalities is not clearly covered. It is also unclear whether confiscation of property can be applied where the owner or possessor has not been identified. The provisional measures to prevent any dealing, transfer or disposal of property subject to confiscation appear to be sound.

20. As a member of the European Union, Estonia implements UNSCRs 1267 and 1373 through relevant EU instruments, which are directly applicable. In addition, the International Sanctions Act (ISA) was enacted in 2010 to set out the general legal framework for the application, implementation and supervision of international sanctions. As a result of Estonia's reliance on EU instruments, which are not always immediately updated following a listing by the Sanctions Committee, the requirement to apply freezing measures without delay is not met. Estonia has not issued a domestic list to apply freezing measures to EU internals. The ISA does not empower Estonia to examine and give effect to the actions initiated under the freezing mechanism of other jurisdictions. Guidance and communication on freezing measures to financial institutions and other persons appear to be adequate. There are no clear publicly-known procedures for un-freezing funds and assets in a timely manner. Further steps are required in order to strengthen FIU supervision of SR III requirements.

21. The FIU is a structurally independent unit within the Police and Border Guard Board. It is the central and exclusive reception point of information on suspected ML and FT activity. It also receives cash transaction reports (CTRs) and processes information related to ML/FT suspicions received from various state authorities and investigative bodies. Foreign FIU requests are treated as STRs. The FIU is adequately structured and has sufficient technical resources to process and analyse information to identify potential ML, associated offences and FT. Adequate guidance on the manner of reporting has been provided to reporting entities. The FIU has ample powers to request and obtain additional information both from other authorities and reporting entities. It has

direct online access to 34 administrative and law enforcement databases. The power to request information from attorneys is, however, subject to some restrictions. Upon detection of elements of a criminal offence, which is broader than ML and FT, an analytical report is disseminated to the public prosecutor. Information is also forwarded to other law enforcement authorities whenever there are no sufficient grounds yet to initiate criminal proceedings. The FIU may, subject to certain restrictions, also disseminate information when formally requested by law enforcement authorities and the courts. Although the FIU operates under strict confidentiality rules, there is a confidentiality risk involved when the FIU queries unregulated persons. Overall, the FIU appears to be conducting its functions in an effective and efficient manner.

22. Since the 3rd round evaluation, the Estonian Tax and Customs Board (ETCB) has been designated as the competent authority controlling the cross-border transportation of cash. The ETCB was found to be adequately resourced and trained. Estonia, as an EU member, applies Regulation (EC) No. 1889/2005 and has adopted a declaration system of EUR 10,000 or more in cash or bearer negotiable instruments at its external EU borders. The ETCB control of goods rules are applied for the purpose of cash declarations. In case of non-declaration, a false declaration or suspicion of ML/FT, a person may be detained at the border along with cash for a maximum period of 48 hours. The temporary detention of cash is not a frequent occurrence. In case of ML/FT suspicion, the case is reported to the Customs Investigation Department and the FIU. The statistics maintained by the ETCB do not give an indication of the ensuing law enforcement outcome following a notification to the FIU. Cash declarations are reported to the FIU twice monthly. Data on cash declarations, false declarations and ML/FT suspicions is routinely maintained by the ETCB. Although the FIU has direct access to the ETCB's database there is no specific legal provision on the cooperation between the two entities. Neither instances of confiscation of cash nor freezing measures in terms of SR. III were reported in relation to transportation of ML/FT related cross-border transportation of cash. The statistics on cash declarations show a reasonable performance of the control regime. However, the lack of systematic international exchange of information, although not formally a requirement, should be addressed.

## 4. Preventive Measures – financial institutions

23. Estonia has taken several legislative and regulatory measures in order to address the main deficiencies identified during the 3rd round evaluation. The supervisory authorities have also issued guidelines to assist financial institutions in complying with their AML/CFT requirements.

24. The MLTFPA provides for a comprehensive framework for the application of CDD measures and requirements with respect to new and developing technologies. While requirements concerning identification and verification of identity of a beneficial owner are broadly in place, the requirement to determine whether the customer is acting on behalf of another person still needs to be included in the MLTFPA. Most financial institutions displayed good knowledge of identification and verification requirements, on-going monitoring, enhanced CDD and the assessment and management of ML/FT risk. Certain financial institutions, other than credit institutions and insurance companies, did not appear to have a solid grasp of beneficial ownership and source of funds requirements.

25. The legal provisions governing record-keeping requirements are largely in line with the FATF Recommendations. The implementation of these provisions also appears to be sound. Nevertheless, there is no provision to ensure that the mandatory record-keeping period may be extended in specific cases upon the request of competent authorities.

26. The legal framework for monitoring complex, unusual large transactions and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations is still deficient. Among other issues identified, in both cases there is no requirement to examine the nature, purpose of these transactions and keep records of the findings of the examination.

27. The reporting obligation for ML suspicions is in line with the FATF requirements. The FT reporting requirement is deemed to be too generic and does not specifically cover the requirement to report suspicions on funds linked or related to terrorism, terrorist acts or by terrorist organisations. Figures provided by the authorities show an acceptable and proportionate level of compliance with reporting rules. The absence of disclosures made by insurance companies, which was identified as a deficiency in the 3rd round, has been addressed. Although, savings and loans associations have not submitted any suspicious transaction reports (STRs), the ML/FT risk in this sector is considered to be low. The evaluation team considers that leaving the initial transaction postponement decision to the reporting entity may negatively impact on the effectiveness of the reporting regime. Guidance on reporting has been provided by the FIU for both ML and FT.

28. AML/CFT supervision and regulation is carried out by the FSA (for those financial institutions it licences) and the FIU (for other financial institutions, which are not subject to the Core Principles). The MLTFPA provides for adequate supervisory powers to monitor financial institutions' compliance with AML/CFT requirements. However, in practice, the FSA exercises the supervisory powers set out under the Financial Service Authority Act which in some instances go beyond the powers under the MLTFPA. The legal framework providing for market entry requirements, including the application of fit and proper tests, was found to be sound and has been used effectively to prevent criminals from owning or controlling financial institutions

29. The FSA conducts its supervision on the basis of a comprehensive risk-based model which determines its supervisory priorities and the annual AML/CFT on-site inspection programme. On-site inspections are carried out according to an internal methodology and include sample testing mainly targeted at high risk customers or determined on the basis of turnover, volume and length of relationship. Off-site monitoring is based on questionnaires which may be either general or targeted specifically at areas of higher risk. The effectiveness of the supervisory programme is reviewed by an independent internal audit department. While the overall supervisory picture of the FSA appears to be positive, the ongoing supervision and monitoring of investment firms, life insurance companies and payment services providers should be subject to additional focus.

30. AML/CFT supervision by the FIU is focussed on ensuring adequate SAR reporting in order to add value to the analytical function of the FIU. On-site supervision is generally undertaken to raise awareness to members of a subsector and to target individual entities selected due to intelligence collected, complaints or SAR reporting behaviour. Less consideration is given to the inherent ML/FT risks of a subsector. There is no internal methodology used by staff in planning or undertaking on-site inspections. Off-site supervision has decreased significantly since 2010. The supervisory staff of the FIU does not appear to be adequate. As a result, the number of on-site and off-site supervision of financial institutions under the FIU's responsibility is not sufficient.

31. A number of deficiencies were identified with respect to the sanctioning regime for breaches of AML/CFT requirements. The range of sanctions is inconsistent across financial institutions. The maximum financial penalties envisaged under the MLTFPA are not sufficiently proportionate, dissuasive and effective. Sanctions available for legal persons that are financial institutions are not available for their directors and senior management. Moreover, the range of sanctions applied in practice by both the FSA and the FIU was found to be narrow.

## 5. Preventive Measures – Designated Non-Financial Businesses and Professions

32. All DNFBPs are covered by the MLTFPA. The application of preventive measures was extended to cover other businesses and professions such as traders, auditors and non-profit associations and NPOs.

33. The CDD and record-keeping requirements and requirements relating to new and developing technologies and monitoring of complex transactions in the MLTFPA, which are applicable to financial institutions, apply equally to DNFBPs. However, some specific provisions apply exclusively

to certain DNFBPs (such as notaries and attorneys). The same deficiencies under Recommendation 5, Recommendation 10 and Recommendation 11 apply under Recommendation 12. Overall, the private sector demonstrated a satisfactory level of awareness and understanding of the CDD and record keeping obligations under the MLTFPA. Most DNFBPs showed awareness of sector-specific and currents risks and vulnerabilities of ML and TF. They also have internal procedures in place. However, some common weaknesses were identified. In particular, it was noted the identification and verification of the source of funds, especially in the case of higher risk customers, presented challenges to all DNFBPs. The same applies to the implementation of the risk-based approach. The weakest sectors appeared to be the real estate intermediaries and dealers in precious metals and stones.

34. The reporting mechanism for financial institutions applies equally to DNFBPs, except for professionals bound by legal privilege in those circumstances where they provide counsel on the client's legal position or represent their client in legal proceedings. The reporting behaviour of DNFBPs is variable, generally without raising any significant concerns. There are however some sectors which are under-reporting, particularly the real estate intermediaries. It is encouraging that Estonian attorneys seem to take their reporting obligation more seriously than in most countries.

35. AML/CFT supervision of DNFBPs falls within the responsibility of the FIU, except for lawyers and notaries who are supervised by the Bar Association and the Ministry of Justice respectively. The Tax and Customs Board is responsible for licensing casinos and has adequate legal and regulatory powers to stop criminals from owning or operating casinos. The supervisory powers available to the FIU under the MLTFPA are applicable to both financial institutions and DNFBP. Although the MLTFPA supervisory provisions are also available to the Bar Association and the Ministry of Justice, they apply supervisory powers set out under the Bar Association Act and the Notaries Act. None of the supervisory authorities conduct supervision on a risk-sensitive basis and the number of onsite and off-site inspections is low. The sanctioning regime under the MLTFPA, with all its deficiencies, also applies to DNFBPs. The number of sanctions imposed on all DNFBPs was found to be low.

## 6. Legal Persons and Arrangements & Non-Profit Organisations

36. The legislative provisions governing the setting up of legal persons have not changed since the 3rd round evaluation. At the time, it was noted that while all legal persons are required to keep share and shareholder registers, their compliance with this obligation was not supervised by any authorities. Additionally, there was no verification of the accuracy and validity of the data in the registers. These deficiencies have not been addressed. In light of this and the deficiencies identified in relation to the implementation of beneficial ownership requirements by financial institutions, it is doubtful whether competent authorities are in a position to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons. On a positive note, the authorities have taken significant measures to improve the online accessibility of information on legal persons held by the registry. Information on legal persons is maintained at the Central Commercial Register, an online service which includes digital data from the commercial register. This includes a visualised business register which allows queries regarding persons related to companies and displays the results as a structure chart or diagram giving a connection between legal persons and natural persons. Market participants confirmed the value of this resource in practice.

37. Since the 3rd round evaluation, a number of measures have been taken to improve the framework governing non-profit organisations. In 2008, the Non-Profit Associations Act was amended to ensure that information on NPOs in the public register is more reliable and transparent and to require NPOs to submit annual accounts and activity reports to the registrar of NPOs. Information on NPOs, including information on the persons who own, control and direct their activities, is publicly available. As a result of an assessment of the NPO sector by the FIU, in 2012 NPOs were included under the scope of the MLTFPA, whenever a cash payment of more than EUR 15,000 is

made to a NPO. NPOs are therefore now subject to some of the preventive measures applicable to financial institutions and DNFBPs. Supervision of NPOs, which falls under the responsibility of the FIU, is still not being conducted effectively. Outreach to the NPO sector is provided through the Network of Estonian Non-profit Organisations. However, the network only covers a fraction of NPOs operation in Estonia.

## 7. National and International Co-operation

38. The Government Committee for Coordination of Issues Concerning the Prevention of Money Laundering and Terrorist Financing serves as the mechanism for cooperation and coordination domestically for the development and implementation of AML/CFT policies and activities. The committee coordinates the drafting of any legislation concerning AML/CFT and monitors the implementation of the MLTFPA. One of the priorities of the committee is the collection and analysis of statistics to detect possible shortcomings in the Estonian AML/CFT regime. On an operational level, the authorities (law enforcement, FIU, Prosecutor's Office and FSA) coordinate domestically on the basis of cooperation agreements. According to the authorities, cooperation takes place on a daily basis. Nevertheless, it was noted that cooperation between the supervisory authorities needs further strengthening.

39. Estonia has signed and ratified the United Nations Convention against Transnational Organised Crime (Palermo Convention), the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the United Nations Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention). There remain some implementation issues in respect of the Conventions. As noted above, there are also shortcomings in respect of the implementation of S/RES/1267 and 1373.

40. Estonia can provide a wide range of mutual legal assistance in investigations, prosecutions and related proceedings concerning money laundering and the financing of terrorism, in application of the multilateral and bilateral agreements to which it is a party or otherwise based on the national framework provisions. However, the application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect of the scope of the TF offence. Estonia appears to respond to requests for assistance in an efficient and effective manner. Informal international cooperation by the FIU with its counterparts appears to be conducted efficiently. No conclusions could be reached on cooperation by the supervisory authorities and law enforcement agencies (LEAs), since no statistical information was made available.

## 8. Resources and statistics

41. In general, all competent authorities involved in the prevention of ML/FT are adequately structured, funded, staffed and provide with sufficient technical and other resources. The FIU supervisory staff was however found to be insufficient to meet the expected demands of its tasks. All staff are required to maintain high professional standards, including standards of confidentiality, and are appropriately skilled. Relevant training on AML/CFT issues is provided on an ongoing basis.

42. Overall, statistics maintained by all Estonian authorities are adequate. However, it was noted that, with respect to ML convictions, the Ministry of Justice does not maintain detailed information on convictions. Further detailed statistics should also be maintained by the ETCB and the FIU to monitor effectiveness, even though not formally required by the FATF Recommendations.

# III. MUTUAL EVALUATION REPORT

## 1. GENERAL

### 1.1. General Information on Estonia

1. This section provides a factual update of the information previously detailed in the third round mutual evaluation report on Estonia covering the general information on the country, its membership in international organisations and key bilateral relations, economy, system of government, legal system and hierarchy of norms, transparency, good governance, ethics and measures against corruption[2].

*Geography and Population*

2. Estonia is a State in the Baltic region of Northern Europe; it borders Latvia to the South, the Russian Federation to the East, Finland across the Baltic Sea to the North and Sweden to the West. The territory of Estonia covers 45,227 km$^2$ and it is divided into fifteen counties (Maakonnad). As of 1 January 2013, the population of Estonia was of 1 286 479 inhabitants, with more than a third living in Tallinn, its capital and largest city. The largest ethnic groups according to the 2011 population census remain the same as at the time of the third evaluation, notably, Estonians (69,8%), Russians (24,8%), Ukrainians (1,7%) and Belarusians (1%).

*International relations*

3. Estonia is a member of the United Nations, NATO, the European Union and in December 2010 it became a member state of the OECD.

*Economy*

4. Estonia adopted the euro with effect from January 2011. Up to 2010, the official currency in Estonia was the kroon (EEK).

5. In the period following the 3rd round mutual evaluation (2008-2009), Estonia suffered an economic downturn. Since 2010, however, the performance of the economy has improved in all sectors and there has been a rise in GDP growth, as well as of the employment rate.

**Table 1: The key economic indicators in Estonia from 2008 – 2012**

| 1 KEY INDICATORS | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|---|
| 1. GDP at current prices (billion EUR) | 16.2 | 13.8 | 14.3 | 16.0 | 17.0 |
| 2. Real growth of GDP (%) | -4.2 | -14.1 | 3.3 | 8.3 | 3.2 |
| 3. GDP per capita at current prices (EUR) | 12 100 | 10 300 | 10 700 | 11 900 | 13 200 |

[2] The reader is referred to the information set out under this section in the Third round detailed assessment report on Estonia (MONEYVAL(2008)32), which was based on the legislation and other relevant materials supplied by Estonia and information gathered by the evaluation team during its on-site visit to Estonia from 3 to 9 February 2008. The report was adopted by MONEYVAL at its 28th Plenary meeting (8 – 12 December 2008).

| | | | | | |
|---|---|---|---|---|---|
| GDP at market prices, PPS per capita (EUR) | 17 200 | 14 700 | 15 500 | 16 900 | 17 500 |
| Consumer price index compared to previous year (%) | 10.4 | -0.1 | 3.0 | 5.0 | 3.9 |
| Unemployment rate** (%) | 5.5 | 13.8 | 16.9 | 12.5 | 10.2 |
| 4. Current account balance (% of GDP) | -9.2 | 2.8 | 2.9 | 1.8 | -1.8 |
| Government Deficit (-)/ Surplus (% of GDP) | -2.9 | -2.0 | 0.2 | 1.2 | -0.3 |

6. According to the World Bank, in 2012 the value of the GDP in Estonia was USD 21.85 billion. Although Estonia's annual average GDP growth slowed to 3.9% in 2012, it remained the strongest in the Euro zone. The inflation rate stood at 4.2% in 2012, a decrease as compared to 2011, where it stood at 5.1%.

7. Estonia's economic international relations are strongly influenced by its geographical position and are therefore developed principally with its neighbouring countries. As concerns exports, the main trade partners are Sweden, Finland and Russia, whilst for imports, the main partners are Finland, Germany and Sweden. Direct foreign investment in Estonia is from the following countries: Sweden (27.6%), Finland (23.3%), Netherlands (10.4%), Norway and Russia (both slightly below 5%).

8. While foreign trade in Estonia was negatively affected by the crisis, in the past years the values have been steadily increasing and have exceeded those prior to the crisis.

**Table 2: Values of foreign trade in the years 2008 - 2012**

| **2** | **2008** | **2009** | **2010** | **2011** | **2012** |
|---|---|---|---|---|---|
| Exports of goods (billion EUR) | 8.470 | 6.487 | 8.743 | 12.014 | 12.550 |
| Imports of goods (billion EUR) | 10.896 | 7.270 | 9.268 | 12.721 | 13.762 |
| Trade balance (billion EUR) | -2.426 | -0.783 | -0.525 | -0.707 | -1.212 |

9. Estonia is characterised by a high level of Internet access and the use of IT in the public and private spheres. The Estonian payment environment is moving steadily towards achieving maximum digitalisation; in 2012 almost 99% of all the domestic payments initiated via banks were carried out through electronic means and the general share of non-cash payments has tallied over 90% since 2001.

*System of Government*

10. Estonia is a parliamentary democratic republic. The head of the state is the president, who is elected by the Parliament for a five-year term.

11. The legislative power is vested in the unicameral parliament, the Riigikogu, which has 101 members elected for a four-year term by proportional representation. There are currently four main

parties represented in the Parliament. The executive power is exercised by the Government which is led by the Prime Minister.

*Legal system and hierarchy of norms*

12. There have been no significant changes in relation to the legal system and hierarchy of norms, the reader is therefore referred to the 3rd round mutual evaluation report (pages 19 – 21, para 64 – 73) in this connection.

*Transparency, good governance, ethics and measures against corruption*

13. According to the Transparency International Corruption Perception Index, Estonia ranked 28th out of 177 countries and territories around the world in 2013. Furthermore, GRECO's 4th round evaluation report on Estonia related to Corruption Prevention in respect of Members of the Parliament, Judges and Prosecutors, published in 2012, noted that Estonia is considered as the least corrupt country in post-communist Europe and that following its accession to the EU, the levels of perceived corruption have further decreased.

14. In its report GRECO notes that the legal framework to prevent and fight corruption applicable to the three above mentioned professional groups was generally satisfactory. On the other hand, some implementation gaps have been identified, including the insufficient application of the rules on conflict of interest, the absence or insufficient definition of ethical principles and rules of conduct, weak supervision of compliance with ethical principles and rules on conflicts of interests and on disclosure of economic interests and the marginal involvement of civil society in corruption prevention.

15. Further to the first Anti-Corruption Strategy "An Honest State", adopted for the years 2004 to 2007, the 2008-2012 Anti-Corruption Strategy was adopted in 2008, followed by the current strategy adopted in October 2013 for the years 2013-2020.

16. In April 2013 Estonia adopted several legislative measures with the aim to counter corruption, including a new Anti-Corruption Act.[3]

17. In the past years, Estonia has invested in the development of an "eGovernment" with a view to ensuring full transparency of the public administration and the Government. Public services are reachable over the Internet by the general public through a State Portal, which acts as a one-stop-shop for the e-services offered by various government institutions.

**General situation of money laundering and financing of terrorism**

18. The statistics provided by the authorities on court decisions related to money laundering show that, other than drug related offences, the most common predicate offences for money laundering are fraud, computer fraud and tax related offenses (both domestic and foreign).

19. Information obtained from threat assessments conducted at an institutional level (mainly by the FIU and the FSA) highlights a number of higher risk areas in Estonia. For instance, business conducted by financial institutions and DNFBPs with customers from certain countries neighbouring Estonia is considered to pose one of the highest ML risks. In recent years, the obligated entities considered to be most vulnerable to ML have been payment services providers (including alternative payment services) and traders in precious metals. The FIU has identified a number of money laundering schemes whereby funds obtained from cybercrime committed in neighbouring countries were transferred through the payment services market to Estonian "straw men", withdrawn in cash and physically transported to neighbouring countries. Moreover, one of the current trends identified by the authorities is the use of currency exchange offices for the

[3] In May 2014 a new fully digital system was introduced for declarations of interests made by public officials. This system enables the public to access such declarations.

purpose of cashing the funds. Since 2010 the FIU has identified an additional scheme whereby companies registered in Estonia carry out large sale transactions of scrap gold, exchanging the funds received from the sale immediately into cash, in order to launder proceeds generated by tax-fraud offences. To mitigate this emerging risk, in 2012 the authorities included the entities undertaking transactions with gold in the list of obligated persons. The results of the institutional threat assessments also indicated that the widespread use of IT in Estonia increases the ML/FT risk within the financial sector.

20. Though according to the evaluators some sectors clearly under-report suspicious activity, generally the number of reports to the FIU has considerably increased since 2007, from slightly over 5,000 to between 12,000 and 15,000 reports after 2008. The statistical figures over the last three years on the output of SARs and CTRs against the input of the number of disclosures to the FIU also indicate a substantial increase in terms of quantity.

21. As has been mentioned above, Estonia is a highly technically developed country, where the majority of the population commonly uses Internet for daily purposes and almost all transactions are therefore carried out through electronic means. As most of the transactions are not cash-based, large cash transactions are frequently associated with financial and tax money laundering schemes. To mitigate this risk, the Estonian authorities have amended the MLTFPA and have set a threshold for reporting cash transactions to the FIU by the obliged entities.

22. According to Europol's 2013 Terrorism Situation and Trend Report, Estonia is one of the countries in Europe least affected by terrorism threats. Furthermore, the Estonian Internal Security Service attests that there were no active terrorist groups in Estonia in 2012, nor supporters of international terrorist organisations. As concerns the financing of terrorism or any other offences connected with terrorism, no such cases have been identified.

**Table 3: Statistics on the number of recorded criminal offences in the years 2008 - 2012**

| | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|---|
| **CRIMINAL OFFENCES AGAINST PROPERTY** | | | | | |
| Theft (PC Art. 199) | 22,471 | 23,901 | 25,253 | 20,175 | 18,628 |
| Burglary | 3,321 | 3,027 | 3,196 | 2,792 | 2,718 |
| Fraud (Art. 209-213) | 2,649 | 2,634 | 2,472 | 1,724 | 1,682 |
| Robbery | 909 | 726 | 599 | 525 | 457 |
| Theft of vehicles | 1,035 | 934 | 870 | 752 | 620 |
| Concealment[4] | 308 | 399 | 248 | 430 | 517 |
| Other CO against property | 1,616 | 1,605 | 1,416 | 1,302 | 1,304 |
| | | | | | |
| **CRIMINAL OFFENCES of ECONOMIC NATURE** | | | | | |
| Business fraud | 32 | 47 | 18 | 12 | 19 |
| Fraud (Art. 209-213) | 2,649 | 2,634 | 2,472 | 1,724 | 1,682 |
| Issuing of an uncovered cheque, misuse of a credit | N/A | N/A | N/A | N/A | N/A |

[4] There is no specific type of crime as concealment. Nevertheless, there is section 202 in PC (Acquisition, storage or marketing of property received through commission of offence)

| | | | | | |
|---|---|---|---|---|---|
| card[5] | | | | | |
| Tax evasion (PC Art. 386, 389, 389,389) | 96 | 47 | 42 | 43 | 37 |
| Forgery (PC Art. 333-341) | 485 | 522 | 404 | 514 | 437 |
| Abuse of authority or rights (Art. 291) | 52 | 36 | 40 | 32 | 32 |
| Embezzlement (PC Art. 201) | 818 | 903 | 755 | 763 | 801 |
| Usury[6] | N/A | N/A | N/A | N/A | N/A |
| Abuse of Insider Information (PC Art. 398) | 1 | 4 | 2 | 1 | 0 |
| Abuse of Financial Instruments Market (Art. 397-3981) | 1 | 6 | 2 | 1 | 0 |
| Unauthorised Use of Another's Mark or Model (PC Art. 226-227) | 8 | 6 | 15 | 40 | 32 |
| Other CO of economic natures (PC Art.372-402) | 682 | 934 | 1,093 | 1,000 | 763 |
| | | | | | |
| **OTHER CRIMINAL OFFENCES** | | | | | |
| Production and trafficking with drugs (Art. 183-190) | 1,558 | 1,042 | 901 | 913 | 866 |
| Illegal migration (PC Art. 260) | 0 | 2 | 3 | 2 | 5 |
| Production and trafficking with arms (Art. 414-420) | 386 | 325 | 245 | 215 | 275 |
| Falsification of money (Art. 333-333) | 27 | 24 | 14 | 34 | 12 |
| Corruption (Art. 293-298) | 224 | 106 | 129 | 108 | 112 |
| Extortion (Art. 214) | 444 | 370 | 339 | 314 | 290 |
| Smuggling (Art. 391-392) | 363 | 591 | 718 | 549 | 428 |
| Murder, Grievous bodily harm (Art. 113, 114, 118) | 244 | 201 | 187 | 204 | 179 |
| Prohibited Crossing of State Border or Territory, Trafficking in Human Beings (PC Art. 258, 259, Art.133) | 6 | 42 | 32 | 36 | 66+9 |

[5] Already covered by fraud

[6] Usury is not a crime in Estonian legislation.

| | | | | | |
|---|---|---|---|---|---|
| Violation of Material Copyright (PC Art. 222-224) | 46 | 29 | 53 | 31 | 18 |
| Kidnapping, False Imprisonment (Art. 135-136) | 60 | 43 | 44 | 36 | 46 |
| Burdening and Destruction of Environment | 35 | 21 | 27 | 39 | 39 |
| Unlawful Acquisition or Use of Radioactive or Other Dangerous Substances | N/A | N/A | N/A | N/A | N/A |
| Pollution of Drinking Water (PC Art. 403) | 0 | 0 | 0 | 0 | 0 |
| Tainting of Foodstuffs or Fodder | N/A | N/A | N/A | N/A | N/A |
| **TOTAL** | **32,536** | **33,494** | **34,186** | **28,187** | **26,156** |
| **OTHER CRIMINAL OFFENCES (NOT INCLUDED ABOVE)** against life and limb, human rights, honour, sexual integrity, public health, etc. | 18,441 | 14,865 | 14,154 | 14,380 | 14,660 |
| **NUMBER OF ALL CRIMINAL OFFENCES** | **50,977** | **48,359** | **48,340** | **42,567** | **40,816** |

**Overview of the financial sector and designated non-financial businesses and professions**

**Financial sector**

23. Financial institutions operating in Estonia can be classified under the following categories: those licensed by the FSA (including branches of financial institutions from non-EU States); and branches or subsidiaries of European Union financial institutions. These last financial institutions can offer any of the financial services that they have a license for in their country of origin and are subject to the supervision of the supervisory institution of their country of origin. A number of financial institutions (which are not subject to the Core Principles) under the supervision of FIU. These are required to register with the Economic Activity Register before commencing operations in the corresponding area of activity according to Art. 52 of MLTFPA[7]. You can see also from the table below which type of businesses are under supervision of FIU:

**Table 4: Number of financial institutions and details about the supervisory authority**

| **Financial Institutions** | | |
|---|---|---|
| **Type of business** | **Supervisor** | **No. of Registered Institutions** |

[7] Since 1 July 2014 these financial institutions are required to obtain a licence from the FIU rather than simply register.

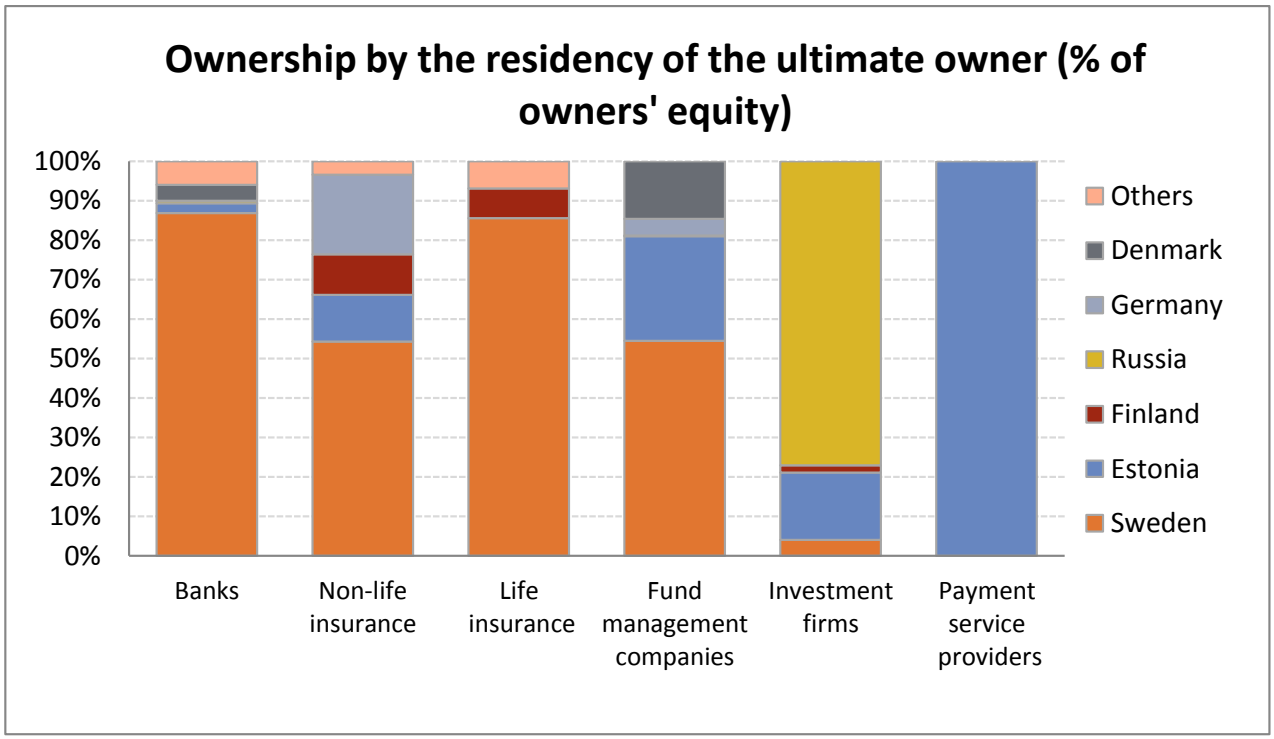
| | | |
|---|---|---|
| 1. Acceptance of deposits and other repayable funds from the public | FSA (credit institutions) | Credit institutions -8<br>Branches of foreign credit institutions – 9<br>Cross-border banking services – 282 |
| | FIU, Bank of Estonia, Savings Guarantee Foundation (Loan and Savings Associations) | Loan and Savings Associations - 8 |
| 2. Lending | FSA (credit institutions) | Credit institutions -8<br>Branches of foreign credit institutions – 9<br>Cross-border banking services – 282 |
| | FIU, Bank of Estonia, Savings Guarantee Foundation (Loan and Savings Associations) | Loan and Savings Associations - 19 |
| | FIU (Consumer Credit Providers) | Consumer credit providers – 198 |
| 3. Financial leasing | FIU (Other financial institutions) | Other financial institutions: leasing - 47 |
| 4. The transfer of money or value | FSA (Payment service providers)(since 2010) | Payment service providers – 8<br>Branches of foreign payment service providers – 0<br>Cross-border payment services – 143 |
| | FSA (E-money institutions)(since 2010) | E-money service providers – 0<br>Branches of foreign payment service providers – 0<br>Cross-border e-money services – 34 |
| 5. Issuing and managing means of payment (e.g. credit and | FIU | Provider of services of alternative means of payment – |

| | | |
|---|---|---|
| debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money) | | 16. |
| 6. Financial guarantees and commitments | N/A | N/A |
| 7. Trading in:<br>(a) money market instruments (cheques, bills, CDs, derivatives etc.);<br>(b) foreign exchange;<br>(c) exchange, interest rate and index instruments;<br>(d) transferable securities<br>(e) commodity futures trading | FSA (Investment Service Providers) | Investment service providers – 5<br>Branches of foreign investment service providers – 0<br>Cross-border investment services – 1604 |
| 8. Participation in securities issues and the provision of financial services related to such issues | FSA (Investment Service providers) | Investment service providers – 5<br>Branches of foreign investment service providers – 0 |
| 9. Individual and collective portfolio management | FSA (Fund Management Company) | Fund management companies – 18<br>Branches of foreign investment service providers – 0<br>Cross-border investment services – 17 |
| 10. Safekeeping and administration of cash or liquid securities on behalf of other persons | FSA (Depositories = Credit institutions) | Depositories - 3 |
| 11. Otherwise investing, administering or managing funds or money on behalf of other persons | FSA (Pension Funds Management) | Pension Funds Management – 6 |
| 12. Underwriting and placement of life insurance and other investment related insurance | FSA (Life Insurance companies) | Life Insurance companies – 4<br>Branches of foreign life insurance companies - 1<br>Cross border life insurance |

| | | |
|---|---|---|
| | | services - 98 |
| 13. Money and currency changing | FIU | 109 |

24. As can be observed from the diagram below, a large share of the financial market in Estonia is owned by foreign countries, in particular Sweden. Russia also presents a high share of ownership, particularly in the investment firms sector.

**Diagram 1: Ownership of financial sector by the residency of the ultimate owner**




*Credit institutions*

25. As at December 2012, there were eight credit institutions licensed by the FSA and nine branches of foreign credit institutions operating in Estonia; Swedish financial institutions have the largest market share. In addition, the aggregate market share of the four biggest banks (Swedbank AS, AS SEB Pank, Nordea Bank Finland Plc Estonian Branch and Danske Bank A/S Estonian Branch) by loan volumes totalled approximately 90%, making the credit institutions market very concentrated.

*Payment and electronic money institutions*

26. Under the Payment Institutions and Electronic Money Institutions Act, which came into force in January 2010, payment institutions are considered financial institutions within the meaning of Art. 5 of the Credit Institutions Act (CrIA). They are companies which primarily provide payment services and which cannot receive deposits or other repayable funds.

27. Under the same act, an electronic money institution is a public or private limited company whose permanent activity is to issue e-money in its name. E-money institutions shall not grant loans out of or secured by the funds received in exchange for e-money.

28. The above-mentioned institutions are subject to the supervision of the FSA, who is also vested with the authority to issue and revoke licences for the exercise of these activities. At the end of 2012, eight payment institutions licensed by the FSA were conducting business in Estonia; three of these have received a special license restricting the offer of their services to Estonia and allowing the application of lower regulative requirements, as well as limiting the volume of mediated payments.

*Securities market*

29. According to the Securities Market Act, participants on the securities market in Estonia are issuers, investors and professional securities market participants. Professional market participants are investment firms, credit institutions, operators of the regulated market, operators of a securities settlement system and other persons prescribed by law. A person must hold an activity license in order to operate as a professional securities market participant.

30. NASDAQ OMX Tallinn (the Tallinn Stock Exchange) is the only regulated secondary securities market in Estonia providing the administration of common electronic trading system necessary for trading, matching of transaction orders, settlement of securities transactions and listing of companies. NASDAQ OMX Tallinn is a self-regulated organisation, issuing and enforcing its own Rules and Regulations and it is licensed and supervised by the FSA of Estonia. NASDAQ OMX Tallinn is a member of Nordic-Baltic stock exchange alliance NOREX.

31. The Estonian Central Register of Securities Act provides for the Estonian Central Securities Depository (ECSD) to maintain the Estonian Central Register of Securities. It is the main register of the state, which administers share registers of all joint stock companies operating in Estonia and all securities and pension accounts opened in Estonia. The register also includes other electronic securities (shares of private limited companies, bonds, etc.) and keeps records of the history of securities transactions.

*Investment firms*

32. At the end of 2012, five investment firms were authorised to operate in Estonia.

*Fund management companies*

33. Compared to their significance on the market at the time of the 3rd round evaluation, the number of fund management companies in Estonia has increased significantly. In December 2012, there were 18 fund management companies and 17 cross-border fund management companies in Estonia, compared to, respectively, 11 and 9 in 2007. Despite the fact that the number of companies has almost doubled in the past five years, the market remains highly concentrated, with 77% of the market share being held by the 4 biggest companies (the leading company being Swedbank Investeerimisfondid with 43%).

*34.* The fund market is dominated by the pension fund management companies, which accounted for 71% in 2012; their market value having increased in total 31%. The equity funds accounted for 15% of the total volume of managed assets, a significant increase presented also the real estate funds.

*Insurance*

35. In December 2012, the Estonian insurance industry included eight non-life insurance companies, four life insurance companies and the Estonian Traffic Insurance Fund. Furthermore, three foreign insurance companies offered non-life insurance services and one foreign insurance company offered life insurance services through their local branches. In addition, a total of 413 providers of non-life insurance services and 97 providers of life insurance services had been entered into the register of providers of cross-border services by the end of 2012.Based on premiums collected in

Estonia, the life insurance market was led by Swedbank Life Insurance SE, which collected almost 37% of total insurance premiums in 2012.

*Savings and loan associations*

36. Savings and loan associations are regulated by the Savings and Loan Associations Act and their scope of activities is limited to taking deposits from their own members and subordination of government loans and foreign aid funds also only to their members. Already during the 3rd round evaluation the market share of Savings and loan associations was assessed as relatively small; since then the number of entities falling under this category has slightly increased. Currently there are 19 savings and loan associations operating on the financial market of Estonia (compared to 14 during the time of the last evaluation).

**Designated non-financial businesses and professions (DNFBPs)**

**Table 5: Number of DNFBPs registered in Estonia in 2013**

| Type of business | Supervisor | No. of Registered Institutions |
|---|---|---|
| 1. Casinos (which also includes internet casinos) | FIU | 18 gambling organisers (games of chance, betting, lottery), including 9 have remote gambling operating permits (internet casinos) |
| 2. Real estate agents | FIU | 44[8] |
| 3. Persons engaged in the buying-in or wholesale of precious metals and precious stones (since 2012) | FIU | 121 |
| 4. Traders when conducting transactions above EUR 15,000 | FIU | not available |
| 5. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to internal‘ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who | Chamber of Notaries | 94 public notaries |
| | Bar Association | 870 lawyers |
| | FIU | 1171 accountants |

[8] Registered as members in the Association of Real Estate Companies of Estonia.

| | | |
|---|---|---|
| may already be subject to measures that would combat money laundering | | |
| 6. Company Service Providers | FIU | 70 |
| 7. Pawnbrokers | FIU | 119 |

*Casinos*

37. Games of chance are regulated by the Gambling Act which entered into force in January 2009. They may not be organised outside of designated gaming sites (casinos) and must be managed by a public limited company or private limited company whose share capital amounts to at least 1,000,000 euros (compared to 127,800 euros at the time of the third round evaluation). Though under the Gambling Act the operator is not required to be established or registered in Estonia, the company's only field of activity must be the organisation of gambling activities. The share capital of the company must be divided into registered shares in order for all the owners of the company to be identifiable; they also have to comply with the fit and proper criteria.

38. For operating games of chance two types of licenses must be obtained: an activity license and an operating permit. To be eligible for these licenses the applicant has to meet specific requirements provided for in the Gambling Act. At the time of the 3rd round evaluation, the licenser for the activity license was the Governmental Commission for the Licenses of Organising the Games of Chances; currently the competent authority for both types of licenses is the ETCB. The Tax and Customs Board remains, however, the supervisory authority for the requirements of the Gambling Act. Activity licences are issued for an unspecified term and are not transferable. Only the holder of an activity licence may apply for an operating permit which specifies the conditions for organising any type of gambling activity, including cases where gambling is organised via Internet or other forms of communications. The operating permit is issued for a maximum of 20 years, depending on the time specified in the written consent for the opening of the gaming location granted by the local rural municipality government or city government of the gaming location.

39. Whereas in the past the Estonian authorities considered that Internet casinos could be in breach of the Gambling Act (though they were not explicitly prohibited under the law), further to the adoption of the new Gambling Act, remote gambling is now explicitly regulated. It is defined as the organisation of gambling in a manner where the outcome of the game is determined by an electronic device and the player can participate in the game by electronic means of communication, including telephone, Internet and media services. The application for an operating permit for remote gambling must specify the address of the location of the server containing the software used for organising remote gambling. Operating permits for remote gambling may be issued for up to five years.

40. Currently there are 18 companies that may legally provide gambling services in Estonia, including the monopoly on lotteries, Eesti Loto AS. 8 of these companies are operating on-line.

*Lawyers*

41. Under the Bar Association Act, the members of the Estonian Bar Association are attorneys at law and clerks acting under their supervision. Only the above mentioned professionals may provide legal services as advocates. The Bar Association keeps a register of its members and exercises the supervision over them; it has 14 permanent staff members, two of whom are responsible for

AML/CFT issues. The Bar reports annually on the visits which have been conducted; by way of example, in 2012, 20 law-firms were supervised by the Bar Association.

42. At the time of the on-site visit, there were 870 members of the Bar Association and 190 law offices (including branches).

43. As not all lawyers have to be members of the Bar Association, all other professionals who provide legal services must register in the commercial register and are subject to supervision by the FIU.

*Notaries*

44. Under the MLTFPA, the Ministry of Justice exercises supervision over the fulfilment of the requirements which public notaries are subject to under the Notaries Act. In practice, the supervision of notaries is conducted by the representatives from the Ministry of Justice (two persons) in cooperation with the representatives of the Chamber of Notaries (one person). Supervision is carried out as periodical inspection over the professional activities of notaries and it may be regular or special. Around ten supervisory visits are carried out annually. The Ministry of Justice also has the authority to impose a disciplinary penalty to a notary, which may be in the form of a reprimand, a fine or removal from office.

45. At the time of the on-sight visit there were 94 public notaries in Estonia, acting either alone or together in offices, and 8 notary candidates.

*Bailiffs and Trustees in Bankruptcy*

46. The Estonian Chamber of Bailiffs and Trustees in Bankruptcy has been established as a legal person in public law further to the entry into force in January 2010 of the Bailiffs Act and of the amendments to the Bankruptcy Act. Further to the new legislation, only members of the Chamber may act as bailiffs or trustees in Estonia.

*Auditors and accountants*

47. The professional activities of an auditor include auditing, business consultancy and performance of other functions assigned to auditors by legislation. A new Auditor's Activities Act entered into force on 8 March 2010 laying out the requirements to exercise the auditing profession, the rules on passing the examination of professional competence, the legal basis for the professional activities of auditors and the organisation of the Board of Auditors.

48. The Board of Auditors is a self-governing professional association of Estonian auditors which organises and supervises the professional activities of auditors, protects the rights of auditors and maintains the list of auditors who have passed the professional examination. The Board of Auditors may impose disciplinary sanctions upon identification of shortcomings during the exercise of its supervision. The bodies of the Estonian Board of Auditors are the general meeting, the management board and the audit committee. The audit committee conducts the supervision and is assisted by relevant permanent employees of The Estonian Board of Auditors.

49. Its members include both auditors as natural persons, as well as auditing companies; only members of the Auditing Board have the right to practice as auditors in Estonia. State supervision over the activities of the Board of Auditors is exercised by the Ministry of Finance. There were 415 auditors on the list of auditors in September 2013.

50. In addition to the Estonian Accountants Association, which has been functioning since 2002, in June 2010 the Association of Estonian Accounting Firms was established whose charter members are 15 of the largest accounting firms in Estonia. The main aim of both Associations is to improve the quality of accounting services as well as to update good practice for providing accounting services and to ensure the quality of the services provided.

*Dealers in precious metals*

51. The activities of dealers in precious metals are regulated by the Precious Metal Articles Act, which defines as dealers in precious metals any undertaking entered in the commercial register or the register of taxable persons having the right to engage in the manufacture, import, wholesale trade or retail trade in articles of precious metals.

52. According to the MLTFPA, persons engaged in the above mentioned activities concerning precious metals, precious metal articles or precious stones (with the exception of precious metals and precious metal articles used for production, scientific or medical purposes) are required to register in the Register Of Economic Activities before commencing operations[9].

53. Dealers in precious metals and stones are subject to the supervision of the FIU for AML/CFT purposes.

*Trust and company service providers*

54. The term "trusts" in Estonian laws refers to a fiduciary relationship, not to trusts as understood in common law systems. .

55. Under the MLTFPA as amended, a provider of trust and company services is a natural or legal person, which provides a third party, in the context of its economic or professional activity, with at least one of the following services:

    a) The foundation of a company or another legal person;

    b) acting as a director 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 the arrangement of assumption of this position by another person;

    c) the permission to use the address of the seat or place of business, including granting the right to use the address as part of one's contact information or for receiving mail as well as providing companies or other legal persons, civil law partnerships or other similar contractual legal arrangements with services relating to the aforementioned;

    d) acting as a representative of a civil law partnership or another such contractual legal arrangement or appointing another person to the position;

    e) acting as a representative of a shareholder of a public limited company or arrangement of representation of a shareholder by another person, except in the event of companies whose securities have been listed in a regulated securities market and with respect to whom disclosure requirements complying with European Community legislation or equal international standards are applied.

56. Only company service providers exist in Estonia. These entities are required to register in the Register of Economic Activities before commencing operations. As of September 2013 70 company services providers were registered, the number having doubled since the last evaluation (in 2007 there were 26 registered entities).

*Pawnbrokers*

57. Pawnbrokers are persons in whose benefit a pledge is established and who sell the pledged property when the claim is not appropriately performed. Pawnbrokers are also subject to obligations under the MLTFPA and are required to register in the Register of Economic Activities. In September 2013 there were 119 pawnbrokers registered in Estonia.

[9] Since 1 July 2014 these entities are required to obtain a licence from the FIU rather than simply register.

**Overview of commercial laws and mechanisms governing legal persons and arrangements**

58. As no significant changes have been made regarding the laws and mechanisms governing legal persons since the last evaluation, please refer for further detail to the 3rd round mutual evaluation report (pages 29 – 30, para 113 – 121).

*The Register*

59. Company registers are now maintained electronically. In 2007 a Company Registration Portal was launched, enabling persons who have an accepted digital identity document to establish a company via Internet. Since 2008 foreign digital signatures are accepted and as of 2010, annual reports and other required documents are to be submitted in a digital form through the eBusiness Register.

60. The entries in the Register are public; everyone therefore may examine the card register and the business files, and obtain copies of registry cards and of documents in the business files.

*Non-profit organisations*

61. The following table shows the numbers of non-profit organisations registered in Estonia in 2013

**Table 6: Number of registered NPOs in Estonia**

| Type of business | Supervisor | No. of Registered Institutions |
|---|---|---|
| a) Associations, registered in the Central Register of Associations | FIU | 29312 |
| b) Foundations, registered in the Foundations Register | FIU | 799 |
| c) Registered churches and religious communities | MoI | 580 |

**Overview of strategy to prevent money laundering and terrorist financing**

*AML/CFT strategies and priorities*

62. On 17 October 2012, the Governmental Committee for the Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing (thereafter, the Governmental Committee; for a description of this Committee, please see analysis under Recommendation 31) decided that an in-depth money laundering and terrorism financing national risk assessment (NRA) would be launched in order to identify the main weaknesses of the current AML/CTF system and to analyse its effectiveness. To this end, a special taskforce from key governmental authorities and supervisory institutions was set up by the Ministry of Finance and representatives of the private sector subject to MLTFPA obligations were invited to give their input. The World Bank Risk Assessment Methodology and its Second Generation Tool will be applied for the purposes of the NRA to understand the sources of the vulnerability faced by the country and to observe and analyse the effects of various policy options. The principal planned outcome is the adoption of an Action Plan laying out the required actions to strengthen the current AML/CFT system[10].

63. In the course of 2010, the "Guidelines for the Development of the Criminal Policy until 2018" were adopted by the Estonian Parliament, in order to co-ordinate actions taken by state agencies in

[10] Estonia plans to complete NRA during 2014.

crime prevention. This strategic document sets out as its main priorities the fight against organised crime, economic crime (including money laundering) and corruption and focuses on the discovery and the confiscation of proceeds of crime. This document also takes into consideration current developments and trends, putting an emphasis on the risks associated with the development of information technology and the increase of cybercrime.

64. On 7 March 2013, the authorities signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (hereinafter Warsaw Convention). The ratification process has been launched and an analysis of the amendments which need to be made to internal legislation in order to bring it in line with the Convention has been carried out.

65. The Laulasmaa Declaration signed by the Minister of Justice and the Minister of Interior in 2005 with a view of setting common priorities for the prosecutor's office and the police forces (such as fighting organised crime, corruption and economic crime, including money laundering and confiscation) has been renewed and updated in 2009, in 2010 and in March 2013.

66. The Governmental and the Advisory Committee on the Prevention of Money Laundering and Terrorist Financing (the Advisory Committee) play key roles in the strategic planning of AML/CFT issues. The first coordinates legislation on prevention of money laundering and terrorist financing and analyses the competence and capacity of relevant institutions. The second submits opinions and proposals to the Governmental Committee regarding the above mentioned issues. The FIU, the FSA and other competent authorities regularly give to the Governmental Committee overviews of the performed risk assessments, which are then taken into consideration when updating policy papers. Following the last evaluation, the Governmental Committee in consultation with the Advisory Committee adopted an action plan to address the deficiencies identified by the Third Round evaluators. The action plan brought about a number of legislative changes which will be described more in depth in the paragraphs below.

67. On 22 October 2008 the Management Board of the FSA approved advisory Guidelines on "Additional Measures for Preventing Money Laundering and Terrorist Financing in Credit and Financial Institutions", which were renewed after 2013 to incorporate more explicitly a risk based approach and reflect the amendments adopted by the FATF to the standards, as well as the proposals made for the new EU Anti-Money Laundering Directive.

68. Given that the Estonian financial sector is characterised by the predominance of subsidiaries or branches of the EU's financial institutions, one of the principal objectives of the FSA is to cooperate with the supervisory authorities of other countries in order to establish an efficient supervisory framework and analyse the risks present in other countries. To pursue this objective the Bank of Estonia, as well as the FSA have concluded multilateral cooperation agreements with institutions responsible for the financial stability of the European Union Member States and a cooperation agreement with the central banks of Sweden, Latvia and Lithuania.

69. In November 2013, the Government adopted the strategy "Fundamentals of Counter-terrorism in Estonia" to combat terrorism. This strategy focuses above all on the improvement of international and inter-institutional cooperation; prevention of the phenomenon of radicalisation and recruitment for terrorism; and the prevention of terrorist financing and related money laundering.

70. In addition to the above mentioned strategic documents and policies, the objectives of law enforcement and other relevant authorities are also set by the "Main guidelines of Estonia's security policy until 2015", the "Fundamentals of Estonia's security policy" and the "Government of the Republic Action Programme 2011-2015". These documents are the bench-marks against which the activity of the police is assessed.

*The institutional framework for combating money laundering and financing of terrorism*

The Financial Intelligence Unit

71. At the beginning of 2013, the FIU was structured as follows: the head of the FIU, two leading specialists, a senior specialist and 2 subunits, the Analysis Division and the Supervision Division (each with 7 officials). The task of the Analysis Division is to analyse and disseminate SARs and CTRs, whilst the Supervision Division is responsible for supervising the activities of obligated persons regarding compliance with the MLTFPA. The Supervision Unit also includes one strategic analyst who is responsible for gathering and analysing statistical data, ML trends and organizing feedback to reporting parties. Since 2012, the FIU, in addition to its responsibility over a number of financial institutions and DNFBPs, also took over the supervision of persons engaged in the trade or wholesale of precious metals and non-profit organisations.

Asset Recovery Bureau

72. Since the 3rd round evaluation, the Asset Recovery Bureau (ARB) is no longer part of the FIU and is a separate bureau within the National Criminal Police. According to the authorities, this decision was taken with a view of integrating asset recovery more deeply with all criminal investigation units within the Police. The mandate of the ARB is to identify and assess criminal assets during criminal investigations, secure freezing orders from the court, carry out confiscation procedures and cooperate with other countries in its area of expertise, train the Police and Border Guard Board the Tax and Customs Board and Estonian Internal Security Service in this respect. Prior to being a separate entity, the ARB was initially part of FIU and afterwards of the Investigations Bureau within the Central Criminal Police. Further to its reorganization, the number of staff has been increased.

The Financial Supervision Authority

73. The FSA exercises supervision over the obligations under the MLTFPA and the FSA Act. As has been mentioned above, since 2010 the FSA exercises supervisory functions over payment service providers and electronic money institutions.

Prosecutor's Office

74. The Prosecutor's Office is a two-level institution, consisting of the Office of the Prosecutor General as the higher body and four district prosecutor's offices. The territorial competence of the Office of the Prosecutor General covers the entire country; whereas the jurisdictions of the district prosecutor's offices are identical to those of the prefectures (described below under paragraph 78). The Prosecutor's Office prosecutes crimes in cooperation with the following investigative bodies: the Police and Border Guard Board, the Estonian Internal Security Service, the Tax and Customs Board, the Estonian Competition Authority, the Environmental Inspectorate and the General Staff of the Defence Forces.

75. One of the tasks of the Office of the Prosecutor General, as a superior body, is to deal with cross-border international crimes of greater importance and international co-operation.

76. Some prosecutors of the Office of the Prosecutor General are specialised in money laundering cases; every district prosecutor's office is staffed with prosecutors specialising in economic crime (including money laundering).

Police and Border Guard Board

77. The Police and Border Guard Board was set up in 2010 by merging the Police Board, the Border Guard Board and the Citizenship and Migration Board. The Police and Border Guard Board is structured as follows: four departments (National Criminal Police, Public Order Police Department, Citizenship and Migration department and Border Guard Department), a centralized support service and four regional units (North, South, East and West Prefectures).

78. In addition to other competencies, the National Criminal Police (NCP) coordinates criminal police surveillance activities and is responsible for exchanging international criminal information. The main investigative directions of the NCP are organised crime, corruption and serious economic crimes, money-laundering, narcotics, IT crimes and transnational crimes. The NCP, as well as the local units, have specialized divisions to investigate economic crimes, including money laundering.

Estonian Internal Security Service

79. The former Security Police Board now carries out its activities under the name of Estonian Internal Security Service. Its role remains unchanged since the 3rd round evaluation and encompasses, inter alia, the prevention of terrorism in Estonia and contributing to international counter-terrorism activities. In this respect, it collects information, conducts security and surveillance operations, assesses hazards and information, carries out pre-trial investigations and develops national and international cooperation.

The Governmental Committee and Advisory Committee

80. In addition to what has already been explained in the paragraphs above, the Governmental Committee is chaired by the Minister of Finance. Representatives from the FIU, ministries, Tax and Customs Board, The Prosecutor's Office, police, Eesti Pank (Bank of Estonia) and FSA are members of this Committee. Its functions include: coordinating legislation on the prevention of money laundering and terrorist financing and analysing the competence and capacity of the related institutions; analysing the implementation of the MLTFPA in force; submitting proposals to the Government to improve measures for the prevention of money laundering and terrorist financing and to amendment the relevant legislation; coordinating international cooperation on prevention of money laundering and terrorist financing. The Governmental Committee adopts activity reports on the actions undertaken and proposing an action plan for next period. It is assisted in its work by the Advisory Committee of Market Participants on Prevention of Money Laundering and Terrorist Financing, which acts as a conduit between the authorities and the private sector, by collecting information from the latter, providing them a forum in which they can give their input for prospective legislation and enhancing mutual communication in relation to the situation on the market. The members of the Advisory Committee are representatives from different associations of entrepreneurs and other obligated persons.

Ministry of Foreign Affairs

81. According to the new ISA, which entered into force in October 2010, the Ministry of Foreign Affairs is responsible for the imposition of international sanctions, in the context of this report this is of particular relevance with regard to freezing orders imposed to persons connected with terrorism.

Register of Economic Activity[11]

82. According to the registration obligation provided under Art. 52 of the MLTFPA, certain obligated persons are required to register in the Register of Economic Activities, maintained by the Ministry of Economic Affairs, before beginning their activity. The registration procedure is governed by the Register of Economic Activities Act in conjunction with the specifications arising from the MLTFPA.

83. The entities obligated to register are the following:

a) financial institutions who are not subject to supervision by the FSA pursuant to Art. 2 of the FSA Act;

b) providers of trust and company services;

[11] Since 1 July 2014 entities are now required to obtain a licence rather than simply to register.

c) providers of currency exchange services;

d) providers of payment services;

e) providers of services of alternative means of payment;

f) pawnbrokers;

g) persons engaged in buy-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes.

Other institutions relevant for the AML/CFT framework

84. Other institutions which are relevant in the AML/CFT framework in Estonia are, inter alia, the ETCB (which covers issues related to taxes, customs and gambling), the National Bank of Estonia, the Ministry of Finance, the Ministry of Interior, the Ministry of Justice, the Central Register of Securities. As there haven't been any significant changes in the competencies of these institutions since the last evaluation, please refer for more detail to the 3rd round mutual evaluation report (pages 32 – 33, para 135 – 141).

**The approach concerning risk**

85. An important development since the third mutual evaluation report on Estonia is the application of a risk-based approach (RBA) in 2008[12] to ensure that measures to prevent or mitigate money laundering and terrorist financing risks are proportionate to the risks which have been identified. The RBA is applied at three levels: at state level, at supervisory level and at obligated persons' level.

86. As mentioned earlier in this section, in 2012 a national risk assessment (NRA) was launched in order to identify the main weaknesses of the current AML/CTF system and to analyse its effectiveness. The principal planned outcome is the adoption of an Action Plan laying out the required actions to strengthen the current AML/CFT system and should be completed during 2014.

Risks identified and how they are reflected in the preventive legislation

87. Some of the risks identified by the authorities in the context of institutional risk assessments include: the widespread use of IT in Estonia, the transfer of proceeds of Internet crimes from other countries to Estonia or via the Estonian financial system, sale of accounts, the use of "straw men" and the reliance on currency exchange offices to cash proceeds of crime. In addition, given that almost all transactions are carried out through electronic means, large cash transactions are frequently associated with financial and tax money laundering schemes. As concerns the obligated entities considered to be most vulnerable to ML, these are payment services providers (including alternative payment services) and traders in precious metals.

88. The Estonian authorities have made clear efforts to reflect the risks inherent to the Estonian financial system in the preventive AML/CFT legislation. For instance, in 2012 the authorities included the entities undertaking transactions with gold in the list of obligated persons. The MLTFPA now sets a threshold for reporting cash transactions to the FIU by obliged entities and since 2006 amendments of the legislation regarding unregulated money transfer services have been enacted.

Risk-based approach in supervision

89. Since MONEYVAL's third assessment report and further to the transposition of the EU's 3d AML/CFT Directive, Estonia has turned to a risk-based supervision model. The FSA notably plans its supervisory activity on the basis of the vulnerabilities identified and the threats associated to the

[12] With the transposition of Directive 2005/60/EC.

obligated persons. Furthermore, the on-site inspections of the FSA and the requirements are tailored to the risk profile and the specific activities of the obliged entities it supervises.

Guidance/instructions provided in relation to the risk-based approach

90. In order to assist financial institutions in applying the risk based approach in their own activities, the FSA has issued Guidelines on "Measures for Preventing Money Laundering and Terrorist Financing in Credit and Financial Institutions" and has provided obligated persons a risk assessment model. The latter instruments provide guidance on how to determine the level of risk posed by a client/person involved in a transaction, as well as how to detect threats and how to measure the vulnerability to each threat.

Risk approach and Due diligence

91. Further to amendments enacted since MONEYVAL's last assessment, the MLTFPA now provides for a risk-based approach in the exercise of CDD (Art.14(3)), including the possibility of simplified CDD (Art.17(1)) and enhanced CDD measures (Art. 19), respectively, in cases of low and high risk of ML or FT.

92. Paragraph 30 of the MLTFPA, together with Minister of Finance Regulation No. 10 on "Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance" also require obliged entities to develop internal Rules of Procedures identifying transactions which can be classified as low or high risk, as well as the requirements and procedures for entering into such transactions.

**Progress since the last mutual evaluation**

93. Since MONEYVAL's third assessment report on Estonia a number of very positive steps have been taken by the Estonian authorities to improve the AML/CFT legal framework and ensure more effective implementation of the provisions.

94. Amendments to the MLTFPA entered into force in December 2009 and in May 2012 and include, inter alia, the express application of the MLTFPA to NPOs, foundations, persons dealing with wholesale purchase and sale of precious stones and metals.

95. The Penal Code has equally been amended in the time-frame under review in order to ensure the implementation of some of MONEYVAL's recommendations made in the third round. Further to these amendments, conspiracy to commit money laundering, the financing of an individual terrorist and the collection of funds for the purpose of terrorist financing are now criminalized respectively, under Art. $394^1$ and Art. $237^3$ of the Penal Code. Draft legislation broadening the remit of extended confiscation provided under the Penal Code has also been submitted to Parliament on 15 August 2013.

96. A new ISA entered into force on 5 October 2010; it sets out the general legal framework for the application, implementation and supervision of international sanctions - including international financial sanctions issued by the European Union, the United Nations, other international organizations or the Government of the Estonia. Its provisions align the Estonian legal framework on freezing and confiscation of terrorist assets more closely to FATF standards and is to be considered a welcome development.

97. Further to amendments of the Customs Act which entered into force on 1 May 2013, Customs may now retain currency or bearer negotiable instruments when there is suspicion of money laundering or terrorist financing. Furthermore, a new draft law was prepared in the course of 2013 and sent to

the Government for its approval to increase the sanctions for failure to declare or for smuggling cash[13].

98. With the entry into force of the Payment Institutions and Electronic Money Institutions Act on 22 January 2010 (transposing Directive 2007/64/EC), the FSA has become the supervisory authority of payment institutions operating and established in Estonia. It therefore authorises payment institutions' control over their activities, including the assessment of fit and proper requirements of applicants and managers and the internal procedures for the prevention of money laundering and terrorist financing. This Act was further amended in 18 July 2011.

99. A new Anti-Corruption Act providing a new system[14] for the declaration of economic interests by public officials, entered into force on 1 April 2013. Real property, registered vehicles owned or used, shares and securities (both in Estonia and abroad), gifts made and received, debts, and claims above a value limit and total income will be subject to declaration by a public official. Entrepreneurship and participation in boards of private law entities, secondary employment and other interests shall also be declared if they involve a remuneration or risk of corruption. Under the new act both the public and the competent authorities will have access to the declarations; thereby improving the transparency in relation to national PEPs (national politically exposed persons).

100. There have also been developments in relation to legislation regulating DNFBPs. The new Bailiffs Act, which entered into force in 1 January 2010, has set up the Chamber of Bailiffs and Bankruptcy Trustees, the members of which are the sole professionals who may serve as bailiffs or trustees in Estonia.

101. Furthermore, the new Auditors Activities Act which entered into force on 8 March 2010 has established the Supervisory Board of Auditors, an independent supervisory authority which ensures that high standards are secured in the field of auditing.

102. On 7th March 2013 Estonia signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198, the Warsaw Convention). The authorities are in the process of analysing and assessing the amendments needed in order to ensure this instrument's ratification in a short time span.

103. Another welcome initiative as has already been duly noted in this report was the launching in 2012 of an in-depth money laundering and terrorism financing national risk assessment (NRA).

104. On 1 April 2009, the FSA issued advisory Guidelines on "Measures for Preventing Money Laundering and Terrorist Financing in Credit and Financial Institutions" which were published on its website and sent to all supervised entities. These Guidelines were updated in 2013 in order to reflect a more risk-based approach.

Institutional changes

105. As already mentioned under the section 'Overview of strategy to prevent money laundering and terrorist financing', the Police and Border Guard Board was set-up in 2010. On 1 September 2011 the Estonian ARB and the Corruption Crime Bureau were set up. The mandate of the Corruption Crime Bureau is to investigate all criminal offences related to corruption in Estonia.

[13] The relevant amended provision is paragraph 391 of Penal Code and relevant amendments were adopted on 14 January 2014 and came into force on 1st February 2014. The amended Penal Code is available in English in official State Gazette:

https://www.riigiteataja.ee/en/eli/511032014001/consolide

[14] The new system was implemented in May 2014. It is fully digitalised, based on a pre-filled matrix in an on-line database.

# 2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

## *Laws and Regulations*

### 2.1. Criminalisation of Money Laundering (R.1)

2.1.1 Description and analysis

***Recommendation 1 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

106. Recommendation 1 was rated LC in the 3rd round based on the following conclusions:

- It was unclear whether money laundering could be prosecuted without a prior or simultaneous conviction for the predicate offence.
- Conspiracy to commit money laundering was insufficiently covered in the legislation.

*Legal Framework*

107. The money laundering offence is criminalised under Art. 394 of the Penal Code by reference to the definition in Art. 4 of the MLTFPA. As indicated in MONEYVAL's third report, it is common practice in Estonia for a *lex generalis* to make an implicit cross-reference to a *lex specialis* without it being a cause for concern for interpretational purposes. Further to the recommendations made in the third round, conspiracy to commit money laundering is now criminalised under Art. $394^1$ of the Penal Code (the amendment entered into force on the 15th of July 2013). Though the ML offence is generally compliant with the physical and material elements of Art. 3 of the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and Art. 6 of the 2000 UN Convention against Transnational Organised Crime (the Palermo Convention), some shortcomings were identified by the evaluator.

*Criminalisation of money laundering (c.1.1 – Physical and material elements of the offence)*

108. The current money laundering offence provided under Art. 394 of PC reads as follows:

*"**Art. 394. Money laundering***

*(1) Money laundering is punishable by a pecuniary punishment or up to 5 years' imprisonment.*

*(2) The same act, if committed:*

*1) by a group;*

*2) at least twice;*

*3) on a large-scale basis, or*

*4) by a criminal organisation,*

*is punishable by 2 to 10 years' imprisonment.*

*(3) An act provided for in subsection (1) of this section, if committed by a legal person, is punishable by a pecuniary punishment.*

*(4) An act provided for in subsection (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution.*

*(5) A court may, pursuant to the provisions of Art. 83 of this Code, apply confiscation of property which was the direct object of the commission of an offence provided for in this section.*

*(6) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Art. 83[2] of this Code."*

109. Article 4 MLTFPA defines money laundering as follows:

***Article 4. Money laundering***

*(1) Money laundering means:*

*1) the concealment or disguise of the true nature, source, location, disposition, movement, right of ownership or other rights related to property derived from criminal activity or property obtained instead of such property;*

*2) conversion, transfer, acquisition, possession or use of property acquired as a result of a criminal activity or property acquired instead of such property with the purpose of concealing or disguising the illicit origin of the property or assisting a person who participated in the criminal activity so that the person could escape the legal consequences of his or her actions.*

*(2) Money laundering also means a situation whereby a criminal activity, as a result of which the property used in money laundering was acquired, occurred in the territory of another state.*

110. The money laundering offence is broadly in line with the Vienna and Palermo Conventions. However, the evaluation team noted one instance where Art. 4 diverges from the ML offence as set out under the Conventions. Art. 6(1)(b)(i) of the Palermo Convention and Art. 3(1)(c)(i) of the Vienna Convention provide that "*the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime*" should be a criminal offence, **"**subject to the basic concepts of its legal system" (Palermo Convention) or "subject to its constitutional principles and the basic concepts of its legal system" (Vienna Convention) [15]. While Art. 4 of the MLTFPA criminalises these acts, Art. 4(1)2 adds the purposive elements of concealing and disguising the illicit origin of the property to acquisition, possession or use, thereby restricting its scope.

111. The authorities referred to Art. 202 of the PC, criminalising the acquisition, storage or marketing of property received through the commission of an offence (the receiving offence), and Art. 215 of the PC, criminalising unauthorised use of a thing, to demonstrate that the acquisition, possession or use of criminal proceeds by third parties is covered without any restrictions. The evaluation team analysed these provisions and was satisfied that Art. 6(1)(b)(i) of the Palermo Convention and Art. 3(1)(c)(i) of the Vienna Convention are covered through a combined reading of Art. 202 and 215 of the PC. With respect to the acquisition or possession of criminal proceeds by the self-launderer, the authorities provided case-law demonstrating that the ne bis in idem principle applies in Estonia. The use of criminal proceeds by the self-launderer is not excluded by the ne bis in idem principle and therefore its application under Art. 4(1)(2) of the MLTFPA is restricted by the additional purposive element of concealing and disguising the illicit origin of the property. According to the authorities this additional purposive element is not interpreted by the courts as restricting the scope of use of proceeds by the self-launderer, although the evaluation team was not convinced. What the court requires in these cases, as confirmed by one case provided

[15] From the 3rd round report and the analysis of the same issue it is not clear which exactly basic concepts of the legal system or which constitutional principles and the basic concepts of the legal system were taken into account when assessing the compliance of these provisions with Vienna and Palermo Conventions. It appears that the approach taken in the third round report accepted the purposive element of concealing and disguising the illicit origin of the property as the result of subject to the basic concepts of its legal system or subject to its constitutional principles and the basic concepts of its legal system without stating the grounds in the analysis. Furthermore the authorities did not indicate which basic concepts of its legal system should be taken into account.

to the evaluation team, is that the use of proceeds for personal purposes by the self-launderer affects the functioning of the economy. Both the legal provision and court practice therefore restrict the scope of use of proceeds by a self-launderer.

*The laundered property (c.1.2) and proving property is the proceeds of crime (c.1.2.1)*

112. The Palermo Convention Art. 2 (d) and the Vienna Convention Art. 1 (q) both define property as: "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets"

113. The current definition of property as provided under Art. 9 of MLTFPA reads as follows:

> *"**Article 9. Property***
>
> *For the purposes of this Act, property is any object as well as a document certifying the right of ownership of such object or other rights related to the object, including an electronic document, and the benefit received from the object."*

114. The definition of property from Art. 9 of MLTFPA appears to be too narrow since the term "object" might be understood as something corporeal and tangible. However, taking into consideration the definition of an "object" under Art. 48 of General Part of the Civil Code as 'things, rights, and other benefits which can be the object of a right', the definition of property appears to be in line with FATF standard. Furthermore, the authorities provided jurisprudence which confirms this conclusion. In the Supreme Court case No. 3-1-1-92-12 (12.11.2012), the Supreme Court explained that the object of confiscation according to Art. $83^2$ of Penal Code (extended confiscation) can be anything, right and other benefit which can be an object of a right (General Part of the Civil Code Act Art. 48). Mortgage (Law of Property Act Art. 325) and restricted real rights (right of security) referred to in Art. 5 (1) of the Law of Property Act, are to be interpreted as assets in the meaning of PC Art. $83^2$. In case No 1-11-9523 (09.09.2011) two securities' accounts were confiscated from a person who was convicted for illicit importation and exportation of prohibited goods or goods requiring a special permit. In case 1-10-15069 (07.12.2010) a securities' account (worth 338 546,4 EUR) was confiscated from a person who was convicted for the PC Art. 255 (criminal organisation), Art. 336 (Use and bringing into circulation of counterfeit revenue stamps), Art. 375 (Violation of procedure for handling of alcohol).

115. The authorities also provided an extract from the Explanatory Memorandum to MLTFPA to the evaluation team. The extract states that "*Art. 9 sets out the definition 'property' for the purposes of MLTFPA. Property has been defined pursuant to Art. 3(3) of Directive III. The definition is more detailed than the definition of property set out in Art. 66 of the General Part of the Civil Code Act (hereinafter the GPCCA), as a result of which it had to be defined separately in the context of this Act. The definition of property contained in this Act includes very different forms of property. In furnishing the definition of property the present components of the definition have been taken into account, adding components which are not part of the definition under the law in force. Property means any object, i.e. thing, right and other benefit, which may be the object of a right, and documents certifying the right of ownership of such an object or other rights relating to the object, including electronic documents, and gains arising from such an object. In the context of money laundering it may be said that economic value is important, but the form of expression thereof is not. Things and rights of no economic value cannot be objects of money laundering."* Concerning the last sentence of this extract, it should be noted that neither the Palermo nor the Vienna Convention explicitly mention economic value when defining property.

116. The authorities also indicated that *"Property (assets) acquired through an offence is primarily considered to be the thing (i.e. the stolen object or money) that came into the possession of the perpetrator as a result of an offence, the assets gained through the realization of proprietary rights (the rights of claim) gained from an offence, as well as the remuneration received for committing the offense and any new property that was purchased with it. Therefore, the Penal Code covers as*

*"assets acquired through an offence" also the property that was acquired through the transformation of the property initially received from the offence and the property that was acquired as a result of an increase of the property acquired through an offence. If assets acquired by an 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 (according to Art. 85 of the PC).*"

117. The authorities stated that in order to commence prosecution for a ML offence, a prior or simultaneous conviction for the predicate offence is not required under the PC and the MLTFPA. Furthermore, the concept of crime has been replaced with that of criminal activity in order to clarify that in order to proceed for an ML offence, a conviction is not required; LEAs and the prosecutors must only have identified the elements of a concrete crime as provided for under the PC, which crime has generated proceeds. This means that LEAs and prosecutors must establish a clear link between a criminal activity that occurred at a certain time and place and the proceeds generated by such activity without having to determine who the perpetrator was or requiring a conviction for that criminal activity. The authorities also explained that training in this connection has been provided to the police, prosecutors and judges. Indeed, the data submitted by the authorities and the meetings held by the evaluation team, convinced it that a prior conviction is no longer needed - a welcome development since MONEYVAL's third report.

118. Criminal activity, however, remains undefined under Estonian law and doubts have been expressed as to its clarity by practitioners. The explanatory memorandum to MLTFPA states only that *'criminal activity' is a sufficiently broad concept and includes a criminal offence as well as participation in a criminal offence*. While the absence of a definition could facilitate prosecutorial work in proving that the property derived from an unspecified criminal activity, this does not happen in practice. The Estonian authorities interviewed during the on-site mission indicated that it is necessary to establish the existence of a concrete criminal offence, even without a known perpetrator, so the concept of criminal activity does not cover any criminal activity but only the concrete known criminal offences. Moreover, its interpretation as described above hinders the prosecution of cases of autonomous ML where the offence of ML is pursued on the basis of circumstantial, objective evidence and in which the underlying predicate offence has not been identified. Indeed, LEAs have confirmed that they pursue investigations of ML only if they have concrete information on the underlying predicate offence. For this reason, in many cases where the predicate offence has been committed abroad and the respective authorities have not cooperated sufficiently, investigations have been discontinued. Furthermore, the judges met in the course of the visit seemed to be unfamiliar with the concept of autonomous ML. The authorities have explained that a pilot case on autonomous ML whereby the predicate offence has not been identified was at the time of the on-site visit pending before the Supreme Court. However, after the on-site visit the authorities confirmed that the Supreme Court rejected the arguments presented by the prosecution with respect to autonomous ML. This raises concerns over evidential thresholds required by the judiciary to establish underlying predicate criminality.

*The scope of the predicate offence (c.1.3) and Threshold approach for predicate offences (c.1.4)*

119. Estonia applies an all crimes approach, all the designated offences under the FATF Recommendations can therefore be predicate offences for money laundering. However, as noted under SR.II, the scope of the terrorist financing offence does not cover all the aspects of Special Recommendation II. To this extent, the full concept of terrorist financing is not a predicate offence for money laundering.

**Table 7: Designated categories of predicate offences**

| Designated categories of offences based on the FATF Methodology | Offence in domestic legislation |
|---|---|
| Participation in an organised criminal group and racketeering; | Art. 255, Art. 256 |
| Terrorism, including terrorist financing | Art. 237-237[3] |
| Trafficking in human beings and migrant smuggling;<br>Sexual exploitation, including sexual exploitation of children; | Art. 133-134, Art. 141-146, Art. 175, Art. 178[1], Art. 179 |
| Illicit trafficking in narcotic drugs and psychotropic substances; | Art. 392, Art. 194, Art. 183-184 |
| Illicit arms trafficking | Art. 392, Art. 93, Art. 414-420 |
| Illicit trafficking in stolen and other goods | Art. 202, Art. 227, Art. 224, |
| Corruption and bribery | Art. 293-298 |
| Fraud | Art. 209-213 |
| Counterfeiting currency | Art. 333-333[1], Art. 340 |
| Counterfeiting and piracy of products | Art. 222-224, Art. 227 |
| Environmental crime | Art. 353-370 |
| Murder, grievous bodily injury | Art. 114, Art. 118, Art. 113 |
| Kidnapping, illegal restraint and hostage-taking | Art. 135, Art. 136, Art. 172, Art. 134 |
| Robbery or theft; | Art. 199, Art. 200 |
| Smuggling | Art. 391, Art. 392 |
| Extortion | Art. 214 |
| Forgery | Art. 333-341 |
| Piracy | Art. 110 |

| | |
|---|---|
| Insider trading and market manipulation | Art. 398, Art. 398[1], Art. 397 |

*Extraterritorially committed predicate offences (c.1.5)*

120. As already indicated in MONEYVAL's third report, predicate offences for ML extend to criminal activity that occurred in another country. The current provisions of the Estonian PC do not pose any obstacles to investigate money laundering if a predicate offence occurred in another country and would have constituted a predicate offence had it occurred domestically. The statistics provided by the authorities on court decisions concerning ML specify whether the predicate offence was committed abroad. Therefore, the evaluation team was satisfied that criterion 1.5 is met.

*Laundering one's own illicit funds (c.1.6)*

121. In Estonia there are no fundamental principles of domestic law which hinder the prosecution of money laundering in cases in which the offender has also committed the predicate offence ("self-laundering"). Reference is made, however, to the considerations expressed under criterion 1.1 whereby ML would not extend to use of property, knowing, at the time of receipt, that such property is the proceeds of crime, unless the purposive element of concealing the illicit origin of the property is satisfied.

*Ancillary offences (c.1.7)*

122. As concerns ancillary offences, attempt, aiding and abetting are provided for under the general part of the PC. Notably, the definition of accomplice under Art. 22 of PC reads as follows:

> ***Article 22. Accomplice***
>
> *(1) Accomplices are abettors and aiders.*
>
> *(2) An abettor is a person who intentionally induces another person to commit an intentional unlawful act.*
>
> *(3) An aider is a person who intentionally provides physical, material or moral assistance to an intentional unlawful act of another person.*
>
> *(4) Unless otherwise provided by Art. 24 of this Code, a punishment shall be imposed on an accomplice pursuant to the same provision of law which prescribes the liability of the principal offender."*

123. Under Art. 25 of PC Attempt is defined as follows:

> **Article 25. Attempt**
>
> *(1) An attempt is an intentional act the purpose of which is to commit an offence.*
>
> *(2) An attempt is deemed to have commenced at the moment when the person, according to the person's understanding of the act, directly commences the commission of the offence.*
>
> *(3) If an act is committed by taking advantage of another person, the attempt is deemed to have commenced at the moment when the person loses control over the events or when the intermediary directly commences the commission of the offence according to the person's understanding of the act.*
>
> *(4) In the case of a joint offence, the attempt is deemed to have commenced at the moment when at least one of the persons directly commences the commission of the offence according to the agreement of the persons.*

*(5) In the case of an omission, the attempt is deemed to have commenced at the moment when the person fails to perform an act which is necessary for the prevention of the consequences which constitute the necessary elements of an offence."*

124. Facilitating and counseling a ML offence appear to be covered by the concept of "mental assistance" under Art. 22 of the PC. In support of this, the authorities provided a case of the Supreme Court No. 3-1-1-97-09 (23.11.2009), where the court stated that assistance can be provided with a physical act (for example, in case of a violent crime, by preventing the victim from leaving); materially (for example, by providing monetary funds or an object that is needed for committing the crime); as well as morally (for example by counseling, assuring perpetrators decision to commit a crime or by giving prior consent for holding or disposal/selling the assets acquired by a crime). Supreme Court Decision of 19.10.2000 No. 3-1-1-94-00 - points 6.4 and 6.5 – if the actions of the accused are strengthening and assuring the intent of the perpetrator, it is to be evaluated as a form of aiding the commissioning of a crime – as an intellectual contribution.

125. To be in line with the recommendations made during the 3rd round evaluation, the authorities have introduced conspiracy to commit ML under Art.394 of the PC[16].

***"Article 394[1] Conspiracy to commit money laundering offence***

*Conspiring to commit money laundering is punishable by a pecuniary punishment or up to one year of imprisonment."*

126. This ancillary offence however, is not defined under the penal code. The authorities indicated that the Explanatory Memorandum to the PC provides a definition of the term "conspiracy" as follows. *Conspiracy, in the context of money laundering, means an act by which a person agrees with another person or persons with the activities that, in case their intentions are fulfilled, either causes or leads to committing a money laundering offence by one or more conspirators, or would, if circumstances that make impossible to commit an offence would not occur. When considering this offence, it is important to keep in mind that an act that is subject of the conspiracy is not completed yet (otherwise Art. 394 of the PC would apply) and it has not yet reached the stage of an attempt (otherwise Art. 394 in conjunction with Art. 25 of the PC would apply). Conspiracy to commit an offence consists of mutually coordinated expressions of will of at least two persons to commit a crime on a more or less fixed circumstances.* It is important to note that in Estonia, an explanatory memorandum is an inseparable and mandatory part of any draft law. This draft law (regarding Art. 394[1] of the PC), together with the explanatory memorandum, was approved and adopted by Parliament and also presented to the practitioners: prosecutors, judges, defence lawyers etc. Consequently, practitioners are aware of the existence of the provision (Art. 394[1] of the PC) and its content/definition.

*Additional element – If an act overseas which does not constitute an offence overseas but would be a predicate offence if occurred domestically leads to an offence of ML (c.1.8)*

*127.* According to Art. 4(2) of the MLTFPA, *ML also means a situation whereby a criminal activity, as a result of which the property used in money laundering was acquired, occurred in the territory of another state.".* Hence, in practice, money laundering also covers a situation where a criminal activity as a result of which the property used in money laundering was acquired occurred in the territory of another state. However, in order to constitute a criminal activity, the activity should be criminal according to local law, even if no person has been actually convicted. Considering the provisions quoted above the evaluators conclude that the requirement of the additional element is not satisfied.

[16] The amendments entered into force on 15 July 2013.

***Recommendation 32 (money laundering investigation/prosecution data)***

128. As already noted in MONEYVAL's third report, data concerning registered offences, convictions, confiscation orders, persons involved and sentences imposed in money laundering cases is maintained by the Ministry of Justice in the framework of general criminal statistics. Additional information such as the underlying predicate offence, whether the latter was committed domestically or abroad, cases of self-laundering etc. is extracted manually, upon request. In addition, the FIU keeps statistics for its internal use in the form of an excel sheet concerning investigations, the amount of property frozen, seized and confiscated, prosecutions, convictions, persons involved, sentences imposed in money laundering cases and the underlying predicate offences. The additional FIU data, once again, is extracted manually from the database of the Ministry of Justice and as explicitly stated to the delegation, does not purport to be complete or correct. Annex 3 provides a detailed presentation of the statistics maintained by the FIU.

**Table 8: Number of investigations, indictments, final convictions and property frozen/seized/confiscated**

| **2009** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Investigations** | | **Prosecutions** | | **Convictions (final)** | | **Proceeds frozen** | | **Proceeds seized** | | **Proceeds confiscated** | |
| | **cases** | **persons** | **cases** | **persons** | **cases** | **persons** | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) |
| **ML** | 63 | NA | 31 | 84 | 10 | 11 | NA | NA | 10 | 353 758 | 6 | 140 396 |
| **FT** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| **2010** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Investigations** | | **Prosecutions** | | **Convictions (final)** | | **Proceeds frozen** | | **Proceeds seized** | | **Proceeds confiscated** | |
| | **cases** | **persons** | **cases** | **persons** | **cases** | **persons** | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) |
| **ML** | 54 | 81 | 34 | 152 | 16 | 51 | NA | NA | 2 | 24 523 | 7 | 464 660 |
| **FT** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| 2011 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Investigations** | **Prosecutions** | | **Convictions (final)** | | **Proceeds frozen** | | **Proceeds seized** | | **Proceeds confiscated** | |
| | **Number of registered crimes** | **cases** | **persons** | **cases** | **Persons** | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) |
| **ML** | 80 | 10 | 59 | 16 | 65 | NA | NA | 3 | 337 135 | 10 | 1 056 436 |
| **FT** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| 2012 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Investigations** | **Prosecutions** | | **Convictions (final)** | | **Proceeds frozen** | | **Proceeds seized** | | **Proceeds confiscated** | |
| | **Number of registered crimes** | **cases** | **persons** | **cases** | **persons** | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) |
| **ML** | 52 | 25 | 63 | 16 | 45 | NA | NA | 4 | 24 791 994 | 9 | 127 697 |
| **FT** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| 2013 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Investigations** | **Prosecutions** | | **Convictions (final)** | | **Proceeds frozen** | | **Proceeds seized** | | **Proceeds confiscated** | |
| | **Number of registered crimes** | **cases** | **persons** | **cases** | **persons** | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) | **cases** | **amount** (in EUR) |
| **ML** | 34 | 19 | 72 | 12 | 27 | N/A | N/A | N/A | N/A | N/A | N/A |
| **FT** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

***Effectiveness and efficiency***

129. Table 8 shows that between 2009 and 2013, 70 final convictions were handed down by courts for money laundering in relation to 199 persons. This data would appear to represent an encouraging result considering the size of the country and the money laundering threats it is exposed to. Nevertheless, an analysis by the evaluation team of the ML convictions achieved shows that further progress is needed in the way of investigating, prosecuting and securing convictions for more complex cases, such as autonomous ML cases.

130. According to statistics[17] broken down by different types of ML (self-laundering, third party and stand-alone ML - see table below), ML convictions are commonly handed down for self-laundering and stand-alone ML. In some self-laundering cases, the ML offence is generally included in the indictment for the predicate offence(s) and both offences (ML and predicate) are prosecuted concurrently. This is also appears to be the case with most third-party ML cases, where the third party launderer is prosecuted concurrently with the persons accused of having committed the underlying offence (who are often also prosecuted for the ML offence). For instance, in one ML case provided to the evaluation team by the authorities, the indictment included charges against one person (Mr. A) accused of drug trafficking and related ML (self-laundering), a second person (Mr. B) accused of drug trafficking (proceeds-generating offence) and a third person (Mr. C) accused of ML (third-party laundering). In this case, the Mr. A and Mr. B generated criminal proceeds through the trafficking of narcotic drugs. The proceeds were laundered by Mr. A and Mr. C through a company in which Mr. A was a director. The funds were deposited into the accounts of the company. A part of the funds was then transferred to the personal accounts of Mr. A and Mr. C in the form of a fictitious salary. Mr. A and Mr. C also hire-purchased a house and rented an expensive car paid for by the drug-trafficking proceeds.

**Table 9: Convictions broken down by type of ML**

| **Number of convictions (cases)** | | | | |
|---|---|---|---|---|
| | **2010** | **2011** | **2012** | **Total** |
| **Self-laundering** | 12 | 7 | 1 | **20** |
| **Third party ML** | 4 | 4 | 0 | **8** |
| **Stand-alone ML** | 3 | 3 | 11 | **17** |
| **Number of convictions (persons)** | | | | |
| | **2010** | **2011** | **2012** | **Total** |
| **Self-laundering** | 20 | 10 | 2 | **32** |
| **Third party ML** | 12 | 28 | 0 | **40** |
| **Stand-alone ML** | 18 | 9 | 37 | **64** |

[17] FIU statistics for 2009-2012 (see Annex 3)

131. Stand-alone ML cases generally follow the same pattern. In these cases the predicate offence (often computer fraud) is committed outside Estonia. The criminal proceeds are transferred to bank accounts in Estonia and either withdrawn in cash through an ATM or remitted to straw men who then physically deliver the cash to another person. The prosecution is always required to identify the underlying predicate offence, although the identity of the perpetrators is not always clear. The evaluation team was informed that it is not generally difficult to identify the predicate offence in these cases (e.g. the bank of the victim of online credit card fraud confirms that the bank account of the victim had been misused). These cases generally involve a larger number of accomplices as evident from the figures in Table 9 above.

132. As concerns autonomous ML, the Estonian authorities interviewed during the on-site mission indicated that it is necessary to establish the existence of a concrete criminal offence, even without a known perpetrator. The concept of criminal activity (as expressed in the ML offence) does not cover any criminal activity but only criminal offences which have been clearly identified by law enforcement authorities. Moreover, its interpretation as described above hinders the prosecution of cases of autonomous ML where the offence of ML is pursued on the basis of circumstantial, objective evidence and in which the underlying predicate offence has not been identified. The judges met in the course of the visit seemed to be unfamiliar with the concept of autonomous ML. The pilot case on autonomous ML whereby the predicate offence has not been identified was at the time of the on-site visit pending before the Supreme Court. However, after the on-site visit the authorities confirmed that the Supreme Court rejected the arguments presented by the prosecution with respect to autonomous ML. This raises concerns over evidential thresholds required by the judiciary to establish underlying predicate criminality.

133. The most common form of laundering prosecuted in Estonia is the transfer of proceeds obtained from a criminal activity for the purpose of concealing the origin of the funds. The use of corporate bank accounts within Estonia appears to be the prevalent ML typology for both domestic and foreign predicate offence. Proceeds are generally co-mingled with the funds of a company and deposited into corporate bank accounts. The proceeds are then either withdrawn in cash or integrated through the purchase of property. The use of straw men as beneficiaries of money remittances from proceeds generated by foreign predicate offences is another common typology. The use of professional money launderers does not feature in the information provided by the authorities. The sentences meted out by the courts for ML do not appear to reflect professional laundering being uncovered. The evaluation team is of the view that, given that a number of ML offences appear to have been committed by criminal groups, this phenomenon may not be receiving sufficient focus by law enforcement authorities, thereby escaping detection.

134. Concerning the level of predicate criminal activity from the statistics provided by the authorities one can note that criminal offences against property (mainly theft, burglary and fraud) are the prevailing type of criminality followed by criminal offences of an economic nature (fraud, embezzlement, forgery etc.). The value of laundered assets is not generally substantial. Besides one case where a ship, a number of vehicles, real estate property and intangible assets were confiscated (the value of which was not provided by the authorities), the highest confiscation order for ML was just over five hundred thousand euro. With respect to other convictions, only four cases involved amounts which exceeded a hundred thousand euro. The others involved cases (9) between twenty thousand euro and eighty thousand euro and cases (11) between 30 EUR and fifteen thousand euro. In those cases where no property was confiscated, it was unclear to the evaluation team what the value of the laundered property was[18]. Sanctions imposed by the courts for ML range from prison sentences of 4 months to 5 years (only 1 with respect to two persons) and the compulsory dissolution of a legal person (see statistics in Annex 3). However, in self-laundering cases (where the person is charged with both the predicate offence and ML), the prison

[18] These figures do not include property confiscated as a result of a civil suit.

sentences are consecutive. Indeed, the evaluation team noted that the average prison sentence handed down by the courts for ML is two years, which appears to be the benchmark used by the judiciary for laundering offences. While the length of the sentences may be appropriate in light of the type of laundering and amounts involved, it is also a reflection of the type of ML cases which are being targeted by law enforcement authorities. The ML convictions achieved so far do not appear to suggest that a major effort has been made in Estonia to pursue serious autonomous ML cases.

135. From the statistics provided and discussions held on-site, it appears that the authorities do not conduct parallel financial investigations in relation to all serious proceeds-generating crimes (such as drug-related crimes) with a view to investigating possible ML, which would increase their effectiveness in detecting possible ML cases. During the on-site, the authorities indicated that investigators that are pursuing drug-related offences are mainly focused on asset recovery (the evaluation team retains some reservations regarding asset-recovery results regarding drug-related offences as expressed in the analysis of Recommendation 3) and since the sanction prescribed for production and trafficking with drugs is more severe than sanction for ML, self-laundering related to drugs is usually not investigated and prosecuted. According to LEAs and the Prosecutor this is due to the fact that drug crimes provide the possibility of confiscating assets. In this respect, the evaluator notes that while this could explain lack of prosecution of cases of self-laundering with drug offences as predicates, it does not justify the absence of prosecutions of third-party laundering of proceeds generated from drug crimes. One of the rationales behind the money-laundering offence is to deprive criminals of the proceeds of crime and instrumentalities; this objective would not be attained if all the proceeds generated from the money laundering offence related to a drug predicate crime were not targeted.

136. Prosecutors responsible for combating financial and organised crime are at least once a year offered a training programme concerning civil law issues that are relevant in the context of private law aspects of money laundering, financial crimes and asset recovery. Special round-table meetings are at least once a year organised for prosecutors specialised on money laundering, corruption and other economic crime. Judges are participating in courses organised by relevant authorities regularly, also in relevant seminaries and courses abroad similarly to prosecutors FIU provides special AML training programmes designed for judges. These training sessions cover latest court practice, fight against ML and TF in general, ML and TF legislation (both national and international), trends and possible threats; freezing and confiscation of proceeds of crime, predicate offences etc.

137. As stated earlier on, the authorities informed the evaluation team that between 2010 and 2012 on a yearly basis, the FIU has held training seminars for prosecutors and judges on combating money laundering and terrorist financing, covering, inter alia, the most common predicate crimes, case studies and the definition of criminal activity. However, concerning the prevailing understanding that for investigating and prosecuting autonomous ML it is necessary to identify the concrete underlying predicate offence, some further training on autonomous ML should be required.

### 2.1.2 Recommendations and comments

***Recommendation 1***

138. MONEYVAL is pleased to note that a number of very positive steps have been taken by the Estonian authorities to improve their AML legal framework and ensure a more effective implementation of the provisions. Indeed, conspiracy to commit a ML offence is now explicitly provided for under the PC; the lack of a prior or simultaneous conviction no longer stands in the way of proceeding for ML; and the number of ML convictions has increased. Nonetheless, the

evaluator deems that amendments to Art. 4 of the MLTFPA should be considered in order to align the physical elements of money laundering offence with Vienna and Palermo Conventions.

139. More specifically, in relation to the acquisition, possession or use of property acquired as a result of criminal activity (…), the authorities should remove the purposive elements of concealing or disguising the illicit origin of the property with respect to use of proceeds by a self-launderer.

140. As a signatory to the Warsaw Convention (CETS 198), Estonia should consider taking legislative measures to implement the provisions of Art. 9 paragraph 6 of the Convention. The judiciary should develop jurisprudence on money laundering as an autonomous offence and convict persons for ML where it is proved that the property originated from a predicate offence, without it being necessary to precisely establish which offence.

141. The authorities should also conduct a review of the ML convictions achieved so far to determine whether the criminalisation of ML is being implemented effectively. In particular, this review should assist the authorities in examining the sentencing practices for ML by the courts and serve as a basis for developing a clear methodology to investigate and prosecute ML cases (with an emphasis on complex, third party and autonomous ML cases).

142. The authorities should continue training prosecutors and judges on evidential thresholds for establishing underlying predicate criminality and confront the judiciary with more cases where it is not possible to establish precisely the underlying offence(s).

143. The authorities should consider conducting more parallel financial investigations in relation to major cases of proceeds-generating crimes with a view to investigating possible ML, which should increase their effectiveness in detecting possible ML cases.

144. Shortcomings in the definition of TF as a predicate offence should be amended.

***Recommendation 32***

145. Statistics on ML/FT investigations, prosecutions and convictions are maintained in accordance with c.32.2(b). Nevertheless, it is strongly recommended that the Ministry of Justice maintains additional information such as the underlying predicate offence, whether the latter was committed domestically or abroad, the sentences handed down, the amounts laundered and whether the convictions were for self-laundering, third party ML, stand alone ML and autonomous ML[19]. This will enable the authorities to determine, to a greater extent, whether Recommendation 1 is being implemented effectively.

### 2.1.3 Compliance with Recommendation 1

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.1** | **LC** | • The purposive elements of concealing and disguising the illicit origin of the property narrows the scope of use in self-laundering cases;<br>• The full concept of terrorist financing is not a predicate offence to money laundering;<br>**Effectiveness**<br>• Concerns over evidential thresholds to establish underlying predicate criminality. |

[19] During the discussion of Estonian IV round report at the MONEYVAL 45 Plenary it was concluded by the Plenary that stand alone ML and autonomous ML are synonymous.

## 2.2. Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and analysis

***Special Recommendation II (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

146. Special Recommendation II was rated PC in MONEYVAL's 3rd round report based on the following conclusions: financing of an individual terrorist was not criminalised; the terrorist financing offence did not cover the collection of funds; the law did not specifically criminalise the collection or provision of funds in the knowledge that they are to be used (for any purpose) by a terrorist organisation or an individual terrorist; some conducts as referred to in Art. 2 of the Terrorist Financing Convention and addressed in the specific UN terrorist conventions were not covered.

*Legal framework*

147. The United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention or TF Convention) entered into force in Estonia on 21 June 2002. The provisions implementing its Art. 2, as well as SR.II of the FATF standards are provided for under Art. $237^3$ (Financing and support of acts of terrorism), 237 (Acts of terrorism), $237^1$ (Terrorist organization) and $237^2$ ( Preparation of and incitement to acts of terrorism) of the Estonian PC.

148. The authorities have informed the evaluation team that following MONEYVAL's third round report, Art. $237^3$ of the PC was amended to comply with the recommendations made by the Committee. More specifically, this article now provides that the financing of an individual terrorist and the collection of funds for the purpose of terrorist financing is punishable (the amendments entered into force on 6 April 2009). The evaluators welcome the legislative developments aimed at aligning the offence of financing of terrorism with international standards; it notes, however, that some technical deficiencies have yet to be properly addressed.

*Criminalisation of financing of terrorism (c.II.1)*

149. The Terrorist financing offence (Art. $237^3$ of the PC) as amended provides:

> **"*Article $237^3$ Financing and support of acts of terrorism and activities directed at it***
>
> *(1) A person who **finances** or knowingly supports in another way the commissioning of a criminal offence provided for in Art. 237, $237^1$ or $237^2$ of this Code, as well as **a terrorist organisation** or a **person whose activities are directed at the commission of a criminal offence provided in Art. 237 of this Code**, and makes available or **accumulates funds knowing that these may be used in full or in part to commit a criminal offence provided for in Art. 237, $237^1$ or $237^2$** of this Code, shall be punished by 2 to 10 years' imprisonment.*
>
> *(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution.*
>
> *(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Art. $83^2$ of this Code."*

150. Article $237^3$ PC therefore punishes a person/legal person

- who finances or supports in another way:

- the committing of acts of terrorism as provided for under Art. 237 PC
- the committing of the offence under Art. 237[1] PC (membership in a terrorist organisation)
- the preparation of and incitement to acts of terrorism as set out under Art. 237[2] PC
- organizations or individuals whose activities are directed at committing a terrorist act.

- as well as *"making available and accumulating*" funds knowing that these may be used in full or in part to commit acts of terrorism, by terrorist organisations or for the preparation of and incitement to acts of terrorism.

151. The evaluation team is satisfied that the current formulation of the provisions as amended criminalises:

- the provision of funds (covered by the concept of financing and making available of funds) with the intention that these should be used or in the knowledge that they are to be used, in full or in part, to carry out a terrorist act, by a terrorist organisation or an individual for any purpose regardless of the use that the latter make of the funds (the law does not specifically require that the funds were actually used to carry out (or attempt) a terrorist act or be linked to a specific terrorist act); and
- the collection of funds (covered by the concept of accumulating) knowing that these may be used in full or part for acts of terrorism, by terrorist organisations for any purpose regardless of the use that the latter make of the funds (the law does not specifically require that the funds were actually used to carry out (or attempt) a terrorist act or be linked to a specific terrorist act) for any purpose

152. It is also important to highlight that the wording used in Art. 237[3] PC is broad enough to encompass both direct and indirect intention (knowing that these *may be* used to commit a criminal offence).

153. Nevertheless, the following aspects do not appear to be covered by the FT offence:

- The *indirect* provision or collection of funds with the unlawful intention that they should be used or in the knowledge that they are to be used to carry out terrorist acts, by a terrorist organisation or by an individual terrorist. In this respect the text of Art. 237[3] criminalises financing or supporting in another way, which, if interpreted broadly, could perhaps cover the indirect provision and collection of funds. In the absence of jurisprudence, however, this conclusion is debatable.
- The collection of funds to be used, in full or in part, by an individual terrorist for any purpose other than terrorist purposes.

154. ***Articles 237[1] (terrorist organizations), 237[2] (Preparation of and incitement to acts of terrorism***) and 237 (Acts of terrorism) of the PC have remained unchanged since the 3rd round report and read as follows:

> ***Article 237[1]. Terrorist organisation***
>
> *(1) Membership in a permanent organisation consisting of three or more persons who share a distribution of tasks and whose activities are directed at the commission of a criminal offence provided in Art. 237 of this Code as well as forming, directing or recruiting members to such organisation is punishable by 5 up to 15 years' imprisonment or life imprisonment.*

*(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.*

***Article 237[2]. Preparation of and incitement to acts of terrorism***

*(1) Organisation of training or recruiting persons for the commission of a criminal offence provided in Art. 237 of this Code, or preparation for such criminal offence in another manner as well as public incitement for the commission of such criminal offence is punishable by 2 to 10 years' imprisonment.*

*(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution."*

***"Article 237 Acts of terrorism***

*(1) Commission of a criminal offence against international security, against the person or against the environment, against foreign states or international organisations or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent or interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by 5 to 20 years' imprisonment or life imprisonment.*

*(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.*

*(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Art. 832 of this Code."*

155. Article 237 partially addresses the terrorist acts provided for in the TF Convention in its Art. 2(1)(a) (acts which constitute an offence under the UN treaties annexed to the Convention) and Art. 2(1)(b) (any other act intended to cause death or serious injury to intimidate a population or to compel a government or international organization to do, or refrain from doing, any act).

156. As concerns acts which constitute an offence under the UN treaties annexed to the TF Convention, as was the case in the third round, some do not appear to be covered under Art. 237 (the terrorism offence)(see Table 10 below). Indeed, some of these offences are penalised under other chapters of the Penal Code, however, they are not referred to under the terrorism offence; it follows that these offences are not covered by the terrorist financing provision. It is possible that financing of these offences could be punishable on the basis of aiding and abetting, attempt or conspiracy. However, in light of the first footnote of the methodology in respect of SR II, the criminalisation of FT solely on the basis of aiding and abetting, attempt or conspiracy is not sufficient. As concerns those offences under the UN treaties annexed to the TF Convention which could be deemed to be covered under Art. 237, it is important to highlight that they are penalised only "*if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population"*. An additional condition must therefore be met under the Estonian Penal Code, whilst the TF Convention requires that the

financing of acts which constitute an offence under the UN Treaties annexed to the TF convention be prohibited unconditionally.

**Table 10: Conventions listed in the Annex of the FT Convention**

| | |
|---|---|
| Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970 | **Ratified on 01.06.2002**<br>**Article 111of the PC** |
| Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation done at Montreal on 23 September 1971 | **Ratified on 01.06.2002**<br>**Article 112of the PC** |
| Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973 | **Ratified on 26.09.1991**<br>**Article 246, 247of the PC** |
| International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979 | **Ratified on 01.06.2002**<br>**Article 135of the PC** |
| Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980 | **Ratified on 01.06.2002**<br>**Not fully covered, since Art. 405 PC does not refer to a conduct described in this Convention** |
| 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 | **Ratified on 01.06.2002**<br>**Not fully covered, since Art. 112 PC does not refer to a conduct described in this Convention** |
| Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988 | **Ratified on 01.06.2002**<br>**Article 110of the PC** |
| 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 | **Ratified on 20.12.2003**<br>**Not fully covered, since Art. 407 PC does not refer to Fixed Platforms located on the Continental Shelf described in this Convention** |
| International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997 | **Ratified on 01.06.2002**<br>**Article 237 of the PC** |

157. As concerns Art. 2(1)(b) of the TF Convention, the acts prohibited thereunder are provided for under Art. 237 of the PC. However, while the TF Convention prohibits these acts if their purpose is "to intimidate a population", Art. 237 requires that they "seriously terrorise the population". The authorities have explained that this wording originates from the implementation of Council Framework Decision 2002/475/JHA on combating terrorism and the Council of Europe Convention on the Prevention of Terrorism, CETS No. 196 and does not have an impact on the standards of proof required by the TF Convention or the FATF standards. This position was accepted by the evaluation team.

158. While the TF Convention defines funds as assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit, Estonian legislation does not provide a definition of funds for the purposes of TF. Authorities explained that the definition of objects in Art. 48 of General Part of the Civil Code (*objects are things, rights, and other benefits which can be the object of a right*) would be applied in the criminal procedure in prosecuting TF. However, lack of jurisprudence makes it impossible to assess the implementation of this provision in practice. The FT offence refers to the making available and accumulation of funds without specifying whether the funds have to originate from a legitimate or illegitimate source. The evaluation team is of the view that absent such distinction in the law, the FT offence covers funds deriving from both legitimate and illegitimate sources.

159. The evaluation team notes that the TF Convention is more detailed in this respect and in the absence of any court decisions it is difficult to conclude whether law enforcement and judicial authorities would apply the provisions in line with FATF standards. As was already suggested in the third round report, it would be beneficial to align the wording of the financing terrorism offence with the language of the TF Convention.

160. Essential Criteria II.1 (d) of the FATF standards requiring that the attempt to commit terrorist financing is criminalised is satisfied as the provisions of the general part of the Penal Code, including those on attempt (Art. 25 of PC) fully apply to the offence of terrorist financing.

161. Criterion II.1(e) of SR.II requires that the following conducts are also criminalised: (i) the participation as an accomplice in TF or in attempted TF, (ii) organizing or directing others to commit TF or attempted TF, and (iii) contributing to the commission of TF or to attempted TF by a group of persons acting with a common purpose. Article 22 of the general part of the Penal Code expressly covers participation as an accomplice to an intentional unlawful act (including TF and attempted TF). With respect to C.II.1(e)(ii) and (iii), the Estonian authorities provided case examples indicating, to the satisfaction of the evaluation team, that organising or directing others to commit a criminal offence and contributing to the commission of the criminal offence are also covered by Art. 21 and 22 of the PC.

*Predicate offence for money laundering (c.II.2)*

162. The Estonian money laundering offence follows an all crimes-approach, thus also terrorist financing can be a predicate offence for money laundering, as far as it is criminalised and bearing in mind the deficiencies identifies in the paragraphs above.

*Jurisdiction for Terrorist financing offence (c.II.3)*

163. Criteria II.3 of the FATF standards requires that Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

164. Article $237^3$ the Penal Code criminalises the financing of offences (terrorist organisations/individual terrorists/terrorist acts) as provided for under the Estonian Penal Code. According to Art. 8 (Applicability of penal law to acts against internationally protected legal rights), regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to any acts committed outside the territory of Estonia if the punishability of the act arises from an international obligation binding on Estonia. Furthermore, Art. 9 of the PC prescribes applicability of penal law to acts against legal rights of Estonia. Both provisions provide a legal basis for prosecuting TF with an international element, in line with provisions of the Estonian PC.

165. However, taking into consideration deficiencies described above, (in relation to collection of funds for individual terrorist), the evaluators remain unsatisfied as to potential lack of criminality in a situation of collection of funds abroad intending and knowing that they be used by an individual terrorist for a purpose considered legitimate under Estonian law (e.g. charitable activity) which may not be considered as a TF offence. In such a case it is questionable under current legislation if criminal proceedings could be initiated in Estonia.

166. The same concerns could be raised in relation with the acts constituting offences in the treaties annexed to the Convention, committed (or to be committed) abroad and which are not covered by the Estonian PC.

167. Furthermore, taking into consideration the fact that financing of some conducts addressed in the specific UN terrorist conventions referred to by Art. 2 of the Terrorist Financing Convention are not covered by the TF criminal offence, and the other conducts which are covered by the TF criminal offence require additional purposive element, it appears that this criterion is only partially met.

*The mental element of the FT (applying c.2.2 in R.2)*

168. It appears that in Estonia criminal intent can generally be inferred from objective factual circumstances. Article 61 CCP - *Evaluation of evidence* provides that (1) no evidence has predetermined weight and (2) a court shall evaluate all evidence in the aggregate according to the conscience of the judges. These provisions appear to reflect the principle of free evaluation of evidence.

*Liability of legal persons (applying c.2.3 & c.2.4 in R.2)*

169. Under Art. $237^3$ (2) the terrorist financing offence, if committed by a legal person, is punishable with a fine or compulsory dissolution. According to the General Part of Estonian Penal Code (Art. 14 (2) prosecution of a legal person does not preclude the prosecution of the natural person who committed the offence. It does not preclude any other sanctions from being imposed where provided by law.

*Sanctions for FT (applying c.2.5 in R.2)*

170. Terrorism financing is punished with imprisonment ranging from 2 to 10 years if committed by a natural person; and as stated above with a fine or compulsory dissolution if committed by a legal person. These penalties are in line with those which are applicable in the European Union and appear to be effective, proportionate and dissuasive. However, since to date no cases have been opened, it is not possible to evaluate its application in practice.

***Effectiveness and efficiency and Recommendation 32 (terrorist financing investigation/prosecution data)***

171. The statistics provided by the Estonian authorities show that a high number of TF SARs were reported to the FIU (1,416 in 2009, 1,000 in 2010, 1,153 in 2011, 1,732 in 2012). The evaluator notes however that these notifications were not followed by investigations, indictments or

convictions. The Estonian authorities informed the evaluation team that there were no sufficient grounds to initiate criminal proceedings.

172. According to the Estonian authorities terrorist financing is not a pressing domestic problem. At the same time, in the course of the interviews held, the evaluators' interlocutors highlighted that the Estonian financial sector may be attractive for the purposes of terrorist financing as it is easy to access on-line as well as efficient and fast. The evaluators consider that this aspect should be reflected in the national risk assessment.

173. In the absence of any criminal investigations for financing of terrorism, an assessment of the effectiveness of the system is not possible.

### 2.2.2 Recommendations and comments

***Special Recommendation II***

174. In the absence of case-law, the evaluation team finds Art. ***237[3]*** of the PC difficult to interpret and requiring some further guidance and clarification. In order to dispel any doubts in relation to its compliance with SR.II, the authorities are strongly encouraged at a minimum to: introduce the collection of funds with the intention that they should be used/in the knowledge that they are to be used by *an individual terrorist* for any purpose other than terrorist purposes; expressly criminalise the *indirect* provision or collection of funds with the unlawful intention that they should be used or in the knowledge that they are to be used to carry out terrorist acts, by a terrorist organisation or by an individual terrorist.

175. Estonian authorities should consider amending the Penal Code so that the financing of all conducts referred to in Art. 2(1)(a) of the TF Convention and addressed in the specific UN terrorist conventions are criminalised, while at the same time, removing the additional purposive element provided under Art. 237 of the PC ("*if committed with the purpose to force the state or an international organisation to perform an act or omission …).*

### 2.2.3 Compliance with Special Recommendation II

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **SR.II** | **PC** | • The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered;<br>• TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Art. 2 (1) (a) since these acts are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Art. 237, an additional purposive element is required which limits the application of TF offence;<br>• TF offence does not cover all situations where a person finances a terrorist act committed abroad. |

## 2.3. Confiscation, freezing and seizing of proceeds of crime (R.3)

### 2.3.1 Description and analysis

***Recommendation 3 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

176. Recommendation 3 was rated LC in the 3rd round based on the following conclusions: Laundered property, where money laundering is the only offence being proceeded with, is not covered by the Estonian mandatory confiscation regime; confiscation of instrumentalities used or intended to be used is non-mandatory and does not apply to money laundering or terrorist financing offences; instrumentalities used or intended to be used in the commission of a crime are not subject to value confiscation; there is no specific legislation concerning the rights of bona fide third parties in case of seizure orders (so far Estonia has to rely on general principles of law), which leaves some uncertainty in this regard.

*Legal framework*

177. In August 2013, draft legislation broadening the remit of extended confiscation was submitted to Parliament[20]. Other than this, legislation on confiscation and provisional measures has remained unchanged since the last evaluation. Notably, the Estonian Penal Code provides for a general regime of confiscation (Art. 83, $83^1$,$83^2$, 84, 85) and special provisions on confiscation for money laundering (Art. 394 (5) (6) PC). Provisional measures, including the freezing and/or seizing of property, to prevent any dealing, transfer or disposal of property subject to confiscation are provided under Art. 142 of the CCP. The confiscation regime applies to ML and all the designated offences under the FATF Recommendations identified as predicates to ML. The deficiencies identified in the criminalisation of the FT may, to a limited extent, restrict the ability to freeze and confiscate property.

178. It follows that, though the legislative framework providing for provisional measures and confiscation is by and large sound, the technical deficiencies identified in the third round evaluation report, including the deficiency mentioned above, are still very much relevant for the purpose of this analysis.

*Confiscation of property (c.3.1)*

179. The discretionary confiscation of laundered property in stand-alone ML cases is provided for under Art. 83 and 394(5) and (6) of the CP and is referred to as the *"substance or object which was the direct object of the commission of an intentional offence"*. Confiscation of laundered property from a non Bona fide third party is also provided for under the provisions.

> ***Article 83. Confiscation of object used to commit offence and direct object of offence***
>
> *(1) A court may apply confiscation of the object used to commit an intentional offence if it belongs to the offender at the time of the making of the judgment or ruling.*

[20] The mentioned draft legislation was adopted and entered into force on 8th of March 2014. Under the new law: a one year imprisonment term (instead of three) is required for the purposes of an extended confiscation order; extended confiscation also applies to the assets of a legal person; it is possible to order the extended confiscation of assets of a third party which have been acquired more than 10 years prior to the commission of a criminal offence of a first degree or five years prior to the commission of a criminal offence of a second degree (against the prohibition to confiscate assets acquired than five years prior to the commission of a criminal offence, currently in force).

*(2)* ***In the cases provided by law, a court may confiscate 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,* ***if these belong to the offender at the time of the making of the judgment and confiscation thereof is not mandatory pursuant to law.***

*(3) As an exception, a court may confiscate the objects or substance specified in subsections (1) and (2) of this section if it belongs to a third person at the time of the making of the judgment or ruling and the person:*

*1) has, at least through recklessness, aided in the use of the objects or substance for the commission or preparation of the offence,*

*2) has acquired the objects or substance, in full or in the essential part, on account of the offender, as a present or in any other manner for a price which is considerably lower than the normal market price, or*

*3) knew that the objects or substance was transferred to the person in order to avoid confiscation thereof.*

*(3[1]) If the object used to commit an intentional offence or direct object of offence was used by the person on the basis of a contract for use or contract of sale with a reservation on ownership, a court many confiscate the proprietary rights of the person arising from that contract.*
*(…)*

***Article 394. Money laundering***

*(…)(5) A court may, pursuant to the provisions of Art. 83 of this Code, apply confiscation of a property which was the direct object of the commission of an offence provided for in this section.*

*(6) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Art. 83[2] of this Code.*

180. The confiscation of proceeds, referred to as "assets acquired through an offence", is mandatory under Art. 83[1] of the PC and can be carried out also in respect to non-bona fide third parties.

**Article *83[1]. Confiscation of assets acquired through offence***

*(1) A court shall confiscate the assets acquired through an offence object if these belong to the offender at the time of the making of the judgment or ruling.*

*(2) As an exception, a court shall confiscate the assets or substance specified in subsection (1) this section if these belong to a third person at the time of the making of the judgment or ruling, and if:*
*1) these were acquired, in full or in the essential part, on account of the offender, as a present or in any other manner for a price which is considerably lower than the normal market price; or*
*2) the third person knew that that the assets were transferred to the person in order to avoid confiscation.*

*(3) The court may decide not to confiscate, in part or in full, property acquired through offence if, taking account of the circumstances of the offence or the situation of the person, confiscation would be unreasonably burdensome or if the value of the assets is disproportionably small in comparison to the costs of storage, transfer or destruction of the*

*property. The court may, for the purpose of satisfaction of a civil action, decrease the amount of the property or assets to be confiscated by the amount of the object of the action.*

181. Under Art. 83 of the PC, confiscation of instrumentalities used in the commission of an offence remains discretionary and, according to the authorities, is ordered on the basis of the nature of the offence and the potential danger which the instrumentality presents to society. Cases where the confiscation of instrumentalities was ordered were provided to the evaluation team.

182. The confiscation of instrumentalities intended for use in the commission of a crime is provided for under the general part of the Penal Code – Art. 83 (2) - in cases where these have been used to "prepare a crime" and subject to the Courts' discretion. As noted in the third round, under Estonian penal law, the preparation of a crime is generally not punishable unless it is explicitly criminalised in the special part of the PC. The preparation of money laundering is sanctioned through Art. $394^1$ (*Conspiracy to commit ML*). Given that the preparation of terrorist financing is not expressly criminalised (Art $237^2$ of the PC criminalises Preparation of and incitement to acts of terrorism prescribed in Art. 237 of the PC, not TF), it follows that the confiscation of instrumentalities intended to be used in the commission of financing of terrorism is not provided for under Estonian law. However, in cases of attempted ML/FT, the confiscation of instrumentalities intended to be used in the commission of laundering or financing of terrorism is provided for.

183. Both in the case of laundered property, proceeds and instrumentalities used or intended to be used for the commission of an offence, confiscation is subject to the requirement that the property belonged to the person at the time of the confiscation order. According to C3.1.1(b) property should be confiscated regardless of whether it is held or owned by a criminal defendant or by a third party. The authorities clarified that if the accused transfers the property to a third person, this property can be confiscated by involving the third party in the criminal proceedings. However, it appears that in cases where accused person dies before the criminal proceedings are final and laundered property, proceeds and instrumentalities used or intended to be used for the commission of an offence are inherited by a third person, this additional requirement restricts the scope of the provision..

184. As concerns value confiscation, Art. 84 of the PC provides the following:

***"Art. 84. Substitution of confiscation***

*If assets acquired by an 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."*

185. The evaluators note that the confiscation of property of corresponding value is provided exclusively for proceeds (assets acquired by the offence). Instrumentalities and laundered property are therefore beyond the remit of the provision as was the case in the third round evaluation.

186. As concerns value confiscation of instrumentalities, the authorities deem that it would not serve any purpose as the rationale behind confiscation of instrumentalities is in itself of a preventative nature. The interviews held with practitioners also corroborate the conclusion that in court practice value confiscation of instrumentalities is not applied.

187. As concerns value confiscation of laundered property, a decision of the Supreme Court (Case No. 3-1-1-97-13) has clarified that under Art. 84 of the PC, value confiscation can be carried out only in respect of "assets acquired through an offence" (proceeds) as per Art. 83(1) and that in a stand-alone ML offence, value confiscation would therefore be limited to the gain obtained through ML (income, benefits or profits) and would thus not encompass the totality of the laundered property.

188. According to the interviews held with judges, the concept of "assets acquired through the offence" may be interpreted broadly to encompass profits, income or benefits gained through the

proceeds of crime; property that is derived from proceeds could therefore be confiscated under Art. $83^1$ of the PC. A number of judgements were provided to the evaluation team to support this view. In the Supreme Court case No 3-1-1-97-13 (31.10.2013), in point 12 of the judgement, the Supreme Court explains, that property derived from money laundering is the property, which has been acquired through money laundering activities (for example benefits gained through conversion of the proceeds of crime; profits gained from the money laundering object or any other financial income etc.) In general there is no basis to assume that property that is the direct object of money laundering is also at the same time property acquired through a money laundering offence in the sense of $83^1$ of the PC. In certain cases, however, it might be the so. This is particularly the case when the perpetrator, as a result of the money laundering offence, acquires all property that was the object of money laundering.

189. In the Supreme Court case No 3-1-1-65-13 (17.06.2013), in point 11 of the judgement, the Supreme Court stresses, that as the Criminal Chamber of the Supreme Court has said previously (for example in the case No 3-1-1-92-12 (12.11.2012), point 13); assets acquired through an offence in the meaning of Art. **$83^2$** (1) of the PC are the direct proceeds of crime and the assets derived from the proceeds of crime. Also, profits gained from an offence and assets acquired on account of such profits have to be considered as assets acquired through an offence in the meaning of Art. **$83^1$** (1) of the PC.

190. Estonian authorities are of the view that there is a possibility to confiscate property, on the basis of Art. $83^1$ (1) of the PC from the perpetrator and on the basis of Art. $83^1$ (2) of the PC from the third person; that the perpetrator has acquired directly through an offence or on account of which the perpetrator has gained any new thing, right, and other benefit which can be the object of a right (General Part of the Civil Code Act Art. 48). The evaluation team accepts this explanation which is supported by jurisprudence.

191. The provision on extended confiscation of assets acquired through criminal offence prescribed in Art. $83^2$ of Estonian PC reads as follows:

> ***"Article $82^2$. Extended confiscation of assets acquired through criminal offence***
>
> *(1) If a court convicts a person of a criminal offence and imposes imprisonment for a term of more than three years or life imprisonment, the court shall, in the cases provided by this Code, confiscate a part or all of the criminal offender's assets if these belong to the offender at the time of the making of the judgment, and if the nature of the criminal offence, the legal income, or the difference between the financial situation and the standard of living of the person, or another fact gives reason to presume that the person has acquired the assets through commission of the criminal offence. Confiscation is not applied to assets with regard to which the person certifies that such assets have been acquired out of lawfully received funds.*
>
> *(2) As an exception, a court may confiscate the assets of a third person on the bases and to the extent specified in subsection (1) this section if these belong to the third person at the time of the making of the judgment or ruling, and if:*
>
> *1) these were acquired, in full or in the essential part, on account of the offender, as a present or in any other manner for a price which is considerably lower than the normal market price, or*
>
> *2) the third person knew that that the assets were transferred to the person in order to avoid confiscation.*
>
> *(3) Assets of a third party which has been acquired more than five years prior to the commission of a criminal offence shall not be confiscated.*

*Provisional measures to prevent any dealing, transfer or disposal of property subject to confiscation (c.3.2) and Initial application of provisional measures ex-parte or without prior notice (c.3.3)"*

192. The provisions on provisional measures to prevent any dealing, transfer or disposal of property subject to confiscation have remained unchanged since the third round. Seizure is therefore still provided under Art. 142 of the Code of Criminal Procedure (CCP) and is defined as follows:

***"Art. 142. Seizure of property***[21]

*(1) The objective of seizure of property is to secure a civil action, confiscation or replacement thereof or fine to the extent of assets. Seizure of property means recording the property of a suspect, accused, convicted offender, civil defendant or third party or the property which is the object of money laundering or terrorist financing and preventing the transfer of the property.*

*(2) Property is seized at the request of a Prosecutor's Office and on the basis of an order of a preliminary investigation judge or on the basis of a court ruling.*

*(3) In cases of urgency, property, except property which is the object of money laundering, may be seized without the permission of a preliminary investigation judge. The preliminary investigation judge shall be notified of the seizure of the property within 24 hours after the seizure and the preliminary investigation judge shall immediately decide whether to grant or refuse permission. If the preliminary investigation judge refuses to grant permission, the property shall be released from seizure immediately.*

*(4) Upon seizure of property in order to secure a civil action, the extent of the damage caused by the criminal offence shall be taken into consideration.*

*(5) A ruling on the seizure of property shall be immediately submitted for examination to the person whose property is to be seized or to his or her adult family member, or if the property of a legal person is to be seized, to the representative of the legal person, and he or she shall sign the ruling to this effect. If obtaining of a signature is impossible, the ruling shall be sent to the person whose property is to be seized or to the representative of the legal person who is the owner of the property to be seized. If property is seized in the courses of performance of a procedural act, the representative of the local government shall be involved in the absence of the responsible person or representative.*

*(6) If necessary, an expert or qualified person who participates in a procedural act shall ascertain the value of the seized property on site.*

*(7) Seized property shall be confiscated or deposited into storage with liability.*

*(…)*

*(11) If the grounds for the seizure of property cease to exist before the completion of pre-trial proceedings, a Prosecutor's Office or preliminary investigation judge shall release the property from seizure by an order or ruling."*

193. Although under the above article seizure is applicable to any object that can be confiscated under the PC, the evaluators consider that the limitations identified in relation to the confiscation of instrumentalities (in particular instrumentalities intended for use) and value confiscation, necessarily impacts on the scope of seizure for the purposes of ML, FT and other predicate crimes. As concerns the standard of proof and the relevant procedure for seizing property, reference is made to the 3d round findings, which remain unchanged. The evaluators were equally satisfied that under Art. 142(5) of the CCP, prior notice to the person subjected to seizure is not required.

*Adequate powers to identify and trace property that is or may become subject to confiscation (c.3.4)*

[21] Article 142 of the CCP was amended. The new version entered into force on 1st July 2014.

194. As already indicated in the third round evaluation report, law enforcement agencies, the FIU and other authorities are given adequate powers to identify and trace property. The CCP (Chapter 3) provides all investigative measures that may be used by investigation and prosecution authorities for gathering evidence in order to trace the proceeds of crime. This includes, in particular, the hearing of witnesses (Art. 68), search (Art. 91), seizure and inspection of documents (Art. 86). Surveillance activities are also provided under the CCP (Chapter 31, Art. 1261-12617) 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.

195. The evaluators welcome the setting up in September 2011 of the ARB, a structural unit of the Central Criminal Police. Its role is, inter alia, to: identify, analyse and assess proceeds of crime and assets that can be confiscated as assets acquired through offence as well as assets confiscated on the basis of extended confiscation; conduct surveillance activities and pre-trial criminal proceedings; conduct confiscation proceedings; train prefectures and investigative bodies in the field of tracing and identifying proceeds of crime; and keep records of confiscated assets. This activity is carried out in relation to criminal cases investigated by the Central Criminal Police, and, if necessary by other investigative bodies. The identification of proceeds of crime was formerly carried out by another unit in the Central Criminal Police staffed with three persons in addition to one staff member per prefecture. The ARB is now staffed with ten persons in the bureau plus nine persons working in the prefectures, specialised in tracing and identifying proceeds of crime, an additional welcome development. It must be borne in mind that other units of the Police can also investigate and trace assets and in doing so they are assisted by Guidelines for the identification, tracing and evaluation of assets, issued by the ARB. However, cases involving an important number of assets, as well as those requiring extended confiscation are usually handled by the ARB as they have received specific training in this connection. The ARB also coordinates the activities of the Police and Border Guard Board in the tracing, identification, as well as seizure of assets in the context of criminal proceedings. This is done in accordance with the statute of the central criminal police, which sets out the responsibilities of the ARB, including coordination of all structural units within the police concerning asset recovery area.

*Protection of bona fide third parties (c.3.5)*

196. As concerns the protection of the rights of bona fide third parties, the current provisions expressly provide for the protection of the rights of bona fide third parties in cases of confiscation (under Art. 85 PC).

197. The provision on Effect of confiscation prescribed in Art. 85 of Estonian PC reads as follows:

> ***Article 85. Effect of confiscation***
>
> *(1) Confiscated objects shall be transferred into state ownership or, in the cases provided for in an international agreement, shall be returned.*
>
> *(2) In the case of confiscation, the rights of third persons remain in force. The state shall pay compensation to third persons, except in the cases provided for in subsections 83 (3) and (4), $83^1$ (2) and $83^2$ (2) of this Code.*
>
> *(3) Before entry into force, the decision of an extra-judicial body or court concerning confiscation has the effect of a prohibition against disposal.*

198. Accordingly, if the authorities have unjustly damaged lawful rights of third parties during the confiscation procedure, compensation is due, except in the cases provided for in subsections 83(3) and $83^1$(4), 83(2) and $83^2$(2) of the PC. Assets of a third party which have been acquired more than

five years prior to committing a criminal offence shall not be confiscated.[22] As concerns the protection of the rights of bona fide third parties in case of seizure, no amendments have been carried out since the adoption of the third report on Estonia. In such case general principles, such as the involvement of third parties in the criminal proceedings (Art. 40(1) of the CCP), would apply. Although in the third report, the authorities had acknowledged this omission and were apparently preparing draft legislation, this lacuna has been remedied through abundant Supreme Court practice (made available to the evaluation team).

199. In relation to seizure of property, third parties may file an appeal with the circuit court and the Supreme Court against a court ruling. Section 384 of the CCP prescribes the right to file appeals against rulings as follows.

*"(1) The parties to a court proceeding and persons not subject to the proceeding have the right to file appeals against a ruling of a county court if the ruling restricts their rights or lawful interests.*

*(2) Persons listed in subsection 344(3) of this Code have the right to file appeals against a ruling of a circuit court and persons not participating in the court proceeding have the right to file appeals against a ruling of a circuit court through an advocate if the ruling restricts their rights or lawful interests."*

200. Furthermore, Art. 17 CCP prescribes that parties to the court proceedings are the Prosecutor´s Office, the accused and his or her counsel and the victim, the civil defendant and third parties. The parties to a court proceeding have all the rights of participants provided for in CCP.

*Power to void actions (c.3.6)*

201. Courts in Estonia may take steps to prevent or void actions, whether contractual or otherwise, where persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation. The assets seized shall be taken out of circulation by prohibition against disposal, or by confiscation or deposition into storage with liability. Before entry into force, the decision of an extra-judicial body or court concerning confiscation has the effect of a prohibition against disposal.

*Additional elements (c.3.7)*

202. Membership in a criminal organisation (consisting of three or more persons who share a distribution of tasks, created for the purpose of proprietary gain and whose activities are directed at the commission of criminal offences) is punishable under Art. 255 PC. The property of the organisation is considered as a means intended to commit a crime and therefore is liable to confiscation.

203. The confiscation system in Estonia is based on criminal conviction and does not allow for civil forfeiture.

204. The PC provides for extended confiscation and the reversal of the burden of proof under Art. $83^2$ as described above.

205. Extended confiscation is mandatory and applied only to certain offences (not all the predicate crimes to ML) if the following cumulative conditions are satisfied: a final conviction; a penalty of imprisonment of more than three years or life imprisonment[23]; the proceeds belong to the offender at the time of the judgement; the nature of the criminal offence, the legal income, or the difference

[22] Since 08.03.2014 (date of enactment) the confiscation shall not be applied to assets of a third party which have been acquired earlier than ten years as of the commission of a criminal offence in the first degree (PC Art. 83-2 (3) 1)).

[23] Prerequisite to apply extended confiscation is imprisonment at least one year or life imprisonment. Before the minimum was 3 years or life imprisonment (also since 08.03.2014).

between the financial situation and the standard of living of the person, or another fact gives reason to presume that the person has acquired the assets through commission of the criminal offence.

***Recommendation 32 (statistics)***

206. As already indicated in the context of R.1, data concerning confiscation orders is maintained by the Ministry of Justice in the framework of general criminal statistics. Statistics on seizure are kept by the investigative bodies. Statistics on seizure in cases investigated by Police and Border Guard Board are kept by ARB. Statistics on confiscations, including extended confiscations is gathered and kept by Ministry of Justice.

207. The Estonian authorities provided the following tables in relation to confiscation and seizure orders:

**Table 11: Confiscation orders**

| | 2008 | | 2009 | | 2010 | | 2011 | | 2012[24]* | |
|---|---|---|---|---|---|---|---|---|---|---|
| | cases | amount (in EUR) | Cases | amount (in EUR) | cases | amount (in EUR) | cases | amount (in EUR) | cases | amount (in EUR) |
| Proceeds confiscated for ML offences (including laundered property) | 0 | 0 | 6 | 140,396 | 7 | 464,660 | 10 | 1,056,436.2 | 9 | 127,696.7 |
| Confiscated laundered property in ML cases | No information | No information | No information | No information | 2 | 192,490.6 | 6 | 727,274.5 + 2 computers, 2 vehicles, 3 real estates, a small ship, a trailer | 3 | 41,824.3 |
| Cases of third-party confiscations in relation to ML[25] | | | | | 0 | 0 | 2 | 1 car, mortgage claim, a vehicle, a trailer, a small ship | 2 | 28,534.4 |
| Extended confiscation of ML (PC Art. $83^2$) | | | | | 0 | 0 | 2 | Golden adornment, 1 computer, 1 car, 1 mortgage claim, shares (worth 32,000 EUR) | 1 | 32,642.6 |
| Property confiscated in drug-related crimes[26] | NA | NA | NA | NA | 78 | 215,760 | 93 | 454,373.9 | 110 | 972,795.9 |
| Property confiscated in other offences[27] | NA | NA | NA | NA | 35 | 343,733 | 24 | 334,164.8 | 39 | 804,547.6 |
| Proceeds confiscated (all)[28] | 100 | 918,627 | 142 | 668,673 | 120 | 1,024,153 | 127 | 1,844,974.9 | 158 | 1,905,040.2 |

[24] Starting from the year 2012 the data includes also the value of the assets confiscated (i.e. cars, real estate etc.) , in the preceding years the amounts (in EUR) represent only the value of money confiscated.

[25] ML confiscations where assets have been confiscated from a third person (PC Art. 83 (3), $83^1$ (2), $83^2$ (2)).

[26] Including money as an object of a crime.

[27] Including money as an object of a crime.

[28] Including money as an object of a crime.

208. In addition to the above data, the authorities provided the following examples of confiscated instrumentalities. The following list is not complete but serves to demonstrate the effectiveness of the regime.

- Case No 1-10-2651 (19.03.2010) a car was confiscated (Art. 212 Insurance Fraud)
- Case No 1-09-3576 (10.03.2010) computers were confiscated (Art. 206 Interference in computer data; Art. 207 Hindering of operation of computer system; Art. 208 Dissemination of spyware, malware or computer viruses)
- Case No 1-09-5003 (13.01.2010) 2 cars were confiscated (Art. 199 Larceny)
- Case No 1-09-5578 (29.03.2010) a computer was confiscated **(Art. 394 Money Laundering)**
- Case No 1-10-8117 (18.06.2010) a car was confiscated (Art. 199 Larceny)
- Case No 1-10-9599 (18.10.2010) digital timers, ventilators, digital thermometers, lamps, a radiator, a water-pump, sprinkling system were confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 188 Illegal cultivation of opium poppy, cannabis or coca shrubs)
- Case No 1-10-9931 (13.09.2010) a computer was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 185 Providing of narcotic drugs or psychotropic substances to persons less than 18 years of age)
- Case No 1-09-11463 (17.03.2010) a mobile phone was confiscated (Art. 185 Providing of narcotic drugs or psychotropic substances to persons less than 18 years of age)
- Case No 1-09-16651 (23.11.2009) a car was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-09-18761 (2.03.2010) a computer and cameras were confiscated (sexual crimes as well as Art. 178 Manufacture of works involving child pornography or making child pornography available)
- Case No 1-09-19825 (7.01.2010) (Art. 189 Preparation for distribution of narcotic drugs or psychotropic substances; Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-09-22140 (9.03.2010) (Art. 189 Preparation for distribution of narcotic drugs or psychotropic substances).
- Case no 1-09-13447 (09.09.2011) a car was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-11-3094 (12.04.2011) a car was confiscated (Art. 199 Larceny)
- Case No 1-10-16100 (30.09.2011) a car was confiscated (Art. 391 Illicit traffic)
- Case No 1-11-11838 (1.11.2011) hard-drives were confiscated (Art. 178 Manufacture of works involving child pornography or making child pornography available)
- Case No 1-11-3059 (3.10.2011) a car was confiscated (Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-11-5725 (27.09.2011) a car was confiscated (Art. 391 Illicit traffic)
- Case No 1-11-8481 (3.08.2011) a car was confiscated (Art. 199 Larceny)
- Case No 1-11-9999 (7.10.2011) a computer was confiscated ((Art. 178 Manufacture of works involving child pornography or making child pornography available)
- Case No 1-10-8497 (13.12.2011) a car was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances)
- Case No 1-11-1317 (28.12.2011) a mobile phone was confiscated (Art. $331^2$ Violation of restriction order)

- Case No 1-12-318 (26.01.2012) a car was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-12-360 (12.12.2012) radio transmitters, GPS, a mobile phone were confiscated (Art. 199 Larceny; Art. 255 Criminal Organisation)
- Case No 1-12-4284 (29.05.2012) a computer and a scanner-printer were confiscated (Art. $333^1$ Counterfeiting money)
- Case No 1-12-5276 (15.10.2012) a car and a trailer were confiscated (Art. 375 Violation of procedure for handling of alcohol; Art. 376 Violation of procedure for handling tobacco products)
- Case No 1-12-7300 (30.10.2012) a car was confiscated (Art. 184 Unlawful handling of large quantities of narcotic drugs or psychotropic substances; Art. 392 Illicit import and export of prohibited goods or goods requiring a special permit)
- Case No 1-12-8971 (21.09.2012) a trailer was confiscated (Art. 391 Illicit traffic)

**Table 12: Seized proceeds**

| | 2008 | | 2009 | | 2010 | | 2011 | | 2012* | |
|---|---|---|---|---|---|---|---|---|---|---|
| | cases | amount (in EUR) | cases | amount (in EUR) | cases | amount (in EUR) | Cases | amount (in EUR) | cases | amount (in EUR) |
| Proceeds seized (ML) | NA | NA | 7 | 233,105 | 5 | 977,959 | 3 | 337,135 | 4 | 24,791,994 |
| Proceeds seized (drug-related crimes) | NA | NA | 47 | 369,897 | 65 | 441,528 | 87 | 683,876 | 109 | 1,526,748 |
| Proceeds seized (other) | NA | NA | 9 | 724,973 | 25 | 1,382,850 | 10 | 1,380,096 | 15 | 1,238,027 |
| **Proceeds seized (all)** | **NA** | **NA** | **63** | **1,327,975** | **95** | **2,802,337** | **100** | **2,401,107** | **128** | **27,556,769** |

**Table 13: Convictions for predicate offences**

| | **Convictions (persons)** | | |
|---|---|---|---|
| | **2010** | **2011** | **2012** |
| Drug-related crimes<br>Article183-190 of the PC | 495 | 487 | 482 |
| Crimes related to bribery and gratuities<br>Article 293-298 of the PC | 61 | 40 | 36 |
| Tax crimes<br>Article 386-393 of the PC | 258 | 319 | 314 |

| | | | |
|---|---|---|---|
| *incl. illicit traffic*<br>*Article 391 of the PC* | 138 | 185 | 173 |
| Fraudulent conduct<br>Article 209-213 of the PC | 377 | 386 | 435 |
| Computer crimes<br>Article 206-208 of the PC | 1 | 2 | 4 |

***Effectiveness and efficiency***

209. The statistics provided by the authorities on assets confiscated in relation to ML, FT and predicate offences, when compared to the data made available on the number of convictions for ML, FT and predicate offences, reveal that confiscation is ordered and secured in around 9% of all cases. The percentage reflects the total number of convictions for underlying predicates and ML against the overall number of confiscations per year. However, the Estonian authorities pointed out that the percentage of ML convictions where confiscation was ordered is 44% in 2010, 62.5% in 2011 and 56% in 2012. The evaluators noted that in 2012 there were 306 court decisions in which at least one person was convicted for drug-related crimes (PC Art. 183-189). However confiscation of assets was ordered only in 110 drug-related cases (36%). The evaluation team therefore concluded that while confiscation of assets in ML cases appears to be more regularly utilised, this is not entirely the case with respect to proceeds-generating crimes more generally. The low figures indicate that confiscation is not used as a central tool for combating predicate offences.

210. From a review of a number of ML convictions provided by the authorities, the evaluators noted that the amount of funds being confiscated is low[29]. While the statistics on confiscation orders in Table 11 show that the amount of proceeds confiscated for ML (including laundered property) has steadily increased since 2008 (0.00 EUR in 2008, 140,396.00 EUR in 2009, 464,660.00 EUR in 2010 and 1,056,436.20 EUR in 2011, with a significant decrease in 2012 (127,696.70 EUR)), the evaluation team still considers the figures to be low. The authorities pointed out that since 2012, the statistics also include the value of the assets confiscated (i.e. cars, real estate etc.) while in the preceding years, the amounts (in EUR) represent only the value of money confiscated. Additionally, the authorities pointed out that in those cases which involved victims being deprived of their property, the authorities sought to re-establish the position before the predicate offence occurred. The figures of funds returned to the victims on the basis of a civil claim are not reflected in the statistics on confiscation. .

211. The authorities provided comprehensive statistics on the confiscation of laundered property and examples of cases where the instrumentalities were confiscated. Although the data provided shows that figures still appear to be relatively low (except for instrumentalities), it indicates that some positive progress has been made since the third round evaluation. The number of cases of third-party confiscations in relation to ML remains low as well as the extended confiscation. The evaluation team was informed of two instances in which extended confiscation of assets was ordered in relation to ML in 2011 and one instance in 2012.

[29] Besides one case where a ship, a number of vehicles, real estate property and intangible assets were confiscated (the value of which was not be provided by the authorities), the highest confiscation order for ML was just over five hundred thousand euro. With respect to other convictions, only four cases involved amounts which exceeded a hundred thousand euro. The others involved cases (9) between twenty thousand euro and eighty thousand euro and cases (11) between 30 EUR and fifteen thousand euro.

212. As concerns value confiscation of laundered property, a decision of the Supreme Court (Case No. 3-1-1-97-13) has clarified that under Art. 84 of the PC, value confiscation can be carried out only in respect of "assets acquired through an offence" (proceeds) as per Art. 83(1) and that in a stand-alone ML offence, value confiscation would therefore be limited to the gain obtained through ML (income, benefits or profits) and would thus not encompass the totality of the laundered property.

213. The statistics provided by the authorities in relation to seizures secured in the context of ML and other proceeds-generating crime appear to be adequate. The authorities could provide no specific statistics in relation to seizure of instrumentalities. The legal limitations regarding confiscation of equivalent value assets also have an impact on the seizure of such assets.

214. On a positive note, the setting up in September 2011 of the ARB will ensure greater focus on the identification and tracing of proceeds of crime.

### 2.3.2 Recommendations and comments

215. In order to improve the legislative framework in the field of confiscation and provisional measures, the authorities should ensure that:

- the confiscation of instrumentalities intended to be used in the commission of financing of terrorism is clearly provided for in the law;
- value confiscation of instrumentalities to ML, FT and other predicate crimes and value confiscation of laundered property be expressly provided for under Estonian law.
- confiscation applies to all property subject to confiscation, regardless of whether the owner or possessor has been identified.
- the confiscation of property that is derived from proceeds (i.e. income, profits or other benefits) to be explicitly provided for under the Penal Code, in order to avoid all confusion;
- deficiencies identified in the TF offence (see supra c.II.1) which potentially affect the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organizations and individual terrorists, be remedied.

216. Additionally, more efforts should be undertaken by the authorities to ensure that confiscation is used as a central tool for combating money laundering and predicate offences, through training of investigators, prosecutors and judges. It would also assist if clear policy statements on the priority of confiscation are made to prosecutors in particular by the appropriate senior officials (possibly by the Prosecutor General).

### 2.3.3 Compliance with Recommendation 3

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.3** | **PC** | • Confiscation of property of corresponding value to instrumentalities is not fully provided for;<br>• Confiscation of property of corresponding value to laundered property is not fully provided for;<br>• Unclear whether confiscation of property can be applied where the owner or possessor has not been identified;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for |

| | | |
|---|---|---|
| | | under Estonian law;<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property;<br>• Technical limitations in relation to confiscation of instrumentalities and value confiscation extend to seizure;<br>**Effectiveness**<br>• Low number of confiscation orders with respect to proceeds-generating crime;<br>• Low volume of confiscated assets overall. |

## 2.4. Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and analysis

***Special Recommendation III (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

217. Special Recommendation III was rated PC in the 3rd round based on the following conclusions:

- Estonia did not have a national mechanism to consider requests for freezing from other countries or to freeze the funds of EU internals;
- The definition of funds (deriving from the EU Regulations) did not cover funds controlled by a designated person or persons acting on their behalf or at their direction (as it is required by UNSCRs 1267 and UNSCR 1373);
- Estonia did not have an established national procedure for the purpose of delisting requests.
- No specific procedure for unfreezing the funds or other assets by a freezing mechanism upon verification that the person or entity is not a designated person;
- Apart from banks, no other financial institutions or DNFBP were aware of the procedures to be followed in order to implement the UNSC Resolutions.

*Legal framework*

218. Following Estonia's accession to the EU on 1 May 2004, UN resolutions concerning the freezing of funds and assets of terrorists are implemented through EC legislation, which is directly applicable to its jurisdiction. More specifically, UNSCR 1267 (1999) and its successor resolutions are implemented by Common Position (2002)/402/CFSP and Council Regulation No. 881/2002 of 27 May 2002, whereas S/RES 1373/2001 is implemented by Council Common Positions No. 2001/930/CFSP and No. 2001/931/CFSP on the fight against terrorism and by Council Regulation No. 2580/2001 of 27 December 2001.

219. As concerns UNSCRs 1267 (1999), 1390 (2002), and 1455 (2003), Council Regulation No. 881/2002 imposing certain restrictive measures against the Al-Qaeda and Taliban network, requires the freezing of funds and economic resources belonging to, owned or held by listed individuals or entities and prohibits making available any funds or economic resources to the same. The list of individuals is annexed to the Council Regulation and it is regularly updated by the EU via Commission regulations on the basis of the listing procedure of the Sanctions Committee of UNSCR 1267. Estonia therefore relies on the listing procedure of the EU. On a national level, governmental order No. 477-k (5 August 2003), which clarifies the competences of the Estonian authorities regarding the implementation of Regulation 881/2002, remains in force (for more information on this order refer to the 3rd round MER).

220. UN Security Council Resolutions 1267 (1999), 1390 (2002), and 1455 (2003) are implemented by Council Regulation No. 881/2002 of May 27, 2002, and the most part of S/RES 1373/2001, is implemented by Council Regulation No. 2580/2001 of December 27, 2001.

221. Under UNSCR 1373, member States of the UN are required to have a mechanism in place to determine persons and entities (other than those connected to the Al-Qaeda network) whose funds and assets should be frozen without delay with a view to combating terrorism. Under Council Regulation No. 2580/2001, the Council of the EU has the authority to designate individuals or entities to which the regulation applies and amend or review the list. Member States, however may suggest names to add to the list. Estonia therefore does not have its own separate list but could, under Art.1(1) and (2) together with Art. 7 and 8 of the ISA adopt national implementing measures for the application of international sanctions, thereby complementing the EU list.

***"Article 7 of the ISA***

***National imposition of international sanctions***

*The national imposition of international sanctions shall be decided by an act of the Government of the Republic on the proposal of the Ministry of Foreign Affairs.*

***Article 8. Taking measures***

*(1) On the proposal of the Ministry of Foreign Affairs, the Government of the Republic shall, by an act, take measures for the national imposition of international sanctions and shall amend or repeal them immediately if the act on the imposition of international sanctions is amended, repealed or expires.*"

222. No such measures have been taken to date. Governmental order No 768-k (27 November 2003), which clarifies the competences of the Estonian authorities regarding the implementation of Regulation 2580/2001, remains in force (for more information on this order refer to third round MER).

223. The Council Regulations are directly applicable law in Estonia. Funds and assets are frozen directly and immediately by the Council Regulations.

224. In addition to the above-mentioned supra-national legislation, the ISA entered into force on 5 October 2010. The new ISA sets out the general legal framework for the application, implementation and supervision of international sanctions - including international financial sanctions issued by the European Union, the United Nations, other international organizations or the Government of the Estonia (Art. 3 ISA). Article 1(2) of the ISA states that the objective of the national imposition of international sanctions and the implementation thereof is, in compliance with the United Nations Charter, to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

225. Under its Art. 4 it defines an international financial sanction as:

***"Article 4. International financial sanction***

*(1) For the purposes of this Act, an international financial sanction means a financial sanction that fully or partially prevents a subject of international financial sanction from using and disposing of financial means and economic resources or giving thereof to its possession, inter alia, it is prohibited or restricted:*

*1) to grant a loan and credit or pay financial means on any other similar basis to the subject of international financial sanctions;*

*2) ) to pay any deposits, dividends, interest income and other similar financial means in cash, including by bills of exchange, cheques or other methods and means of payment, also to transfer, pledge securities, precious metals and stones or any other such assets, and give thereof to use or disposal;*

*3) to open a deposit, payment, securities or any other account for a subject of international financial sanctions, give a safe deposit box for their use or enter into contracts for provision of such services;*

*4) to conclude transactions with a subject of international financial sanctions with regard to immovables, registered ships and registered movables or rights;*

*5) to pledge or otherwise give as a security any financial means and economic resources to a subject of international financial sanctions;*

*6) to enter into insurance contracts with a subject of international financial sanctions and make payments on the basis of such contracts;*

*7) to enter into or continue any business relations with a subject of international financial sanctions.*

*(2) The provisions of subsection (1) of this section shall also be applied in the event that the object belongs to the common or joint ownership of several persons of whom at least one is a subject of international financial sanctions."*

226. Under its Art.6, the ISA identifies a number of obligated persons/entities, notably:

*"1) a credit institution within the meaning of the Credit Institutions Act;*

*2) a provider of currency exchange service within the meaning of the Money Laundering and Terrorist Financing Prevention Act;*

*3) an e-money institution within the meaning of the Payment Institutions and E-money Institutions Act;*

*4) a payment institution within the meaning of the Payment Institutions and E-money Institutions Act;*

*5) a provider of alternative means of payment service within the meaning of the Money Laundering and Terrorist Financing Prevention Act;*

*6) an insurer and insurance intermediary within the meaning of the Insurance Activities Act;*

*7) an investment fund established as a management company and a public limited company within the meaning of the Investment Funds Act;*

*8) an account administrator, except an operator of regulated market and an operator of securities settlement system within the meaning of the Estonian Central Register of Securities Act;*

*9) a member of the securities settlement system and an investment firm within the meaning of the Securities Market Act;*

*10) a savings and loan association within the meaning of the Savings and Loan Associations Act;*

*11) other financial institution within the meaning of the Credit Institutions Act;*

*12) a branch of a service provider of a foreign state registered in the Estonian Commercial Register providing the same type of service as the institutions specified in clauses 1)-11) of this section."*

227. Under Art.12(2) of the same act a natural and legal person who has doubts or who knows that a person with whom it is in/about to enter into business relations (…) is the subject of an international financial sanction, must immediately notify the FIU of the identification of the subject or of the doubt thereof and of the measures taken. Under Art. 14(2) of the ISA, he/she is also required to request additional information for identification purposes and; should the latter refuse to provide such information, the obligated person must refuse to enter into the business transaction, apply the international sanction and notify immediately the FIU.

228. Under Art. 13 of the ISA, obligated persons (see Art.6) must: regularly consult the webpage of the FIU, which, under Art.18 of the same act should disclose information about the imposition, amendment or termination of international financial sanctions immediately after receiving the information; check whether the person with whom he/ she is in business relations (…) is subject to an international financial sanction and if so, apply the measure foreseen ; verify whether such international sanction has been repealed and terminate the application of such measure; set-up rules of procedures for the implementation of international financial sanctions and a procedure to supervise its implementation; designate a person in charge of the obligations arising from international financial sanctions.

229. Under Art. 18 of the ISA and Art. 40(1) of the MLTFPA, in the event of suspicion of terrorist financing, the FIU may issue a precept to suspend a transaction and impose restrictions on the disposal of an account or other property constituting the object of the transaction, professional operation or professional service or other assets or property suspected of being associated with terrorist financing for up to 30 days as of the delivery of the precept. In the event of property registered in the land register, ship register, Estonian Central Register of Securities, traffic register, construction register or another state register, the Financial Intelligence Unit may, in the event of justified suspicion, restrict the disposal of the property for the purpose of ensuring its preservation for up to 30 days.

230. Under Art. 18(3) of the ISA if the FIU is notified as per Art. 12 (2), 14 (2) or Art. 19 of the ISA (see below), the FIU must: 1) notify the Ministry of the Interior, the Ministry of Foreign Affairs, and other Ministries, if applicable, of the receipt of the notification or application; 2) verify whether the subject of an international financial sanction has been identified; 3) assess the legality of the measures taken; 4) notify immediately the person who has submitted the notification or application and the ministries of the results of the verification.

231. Under Art. 18(4) of the ISA, if the FIU confirms that the above-mentioned person is subject to an international financial sanction, it must notify the person in writing within two working days of the measures taken as to: 1) the exact scope and content; 2) the legal basis; 3) the date of commencement; 4) the procedure for contestation; 5) the basis and procedure for making exceptions.

232. Under Art. 19 of the ISA a person who has been subject to an international financial sanction may request the FIU to verify immediately if the measures have been taken lawfully.

*Freezing assets under S/Res/1267 (c.III.1)*

233. The legal framework to freeze terrorist funds or other funds of persons designated by the UN Al-Qaida and Taliban Sanctions Committee in accordance with S/RES/1267(1999) has been described in the paragraphs above. Estonia thus relies on EC regulation 881/2002 to implement the list of designated persons and entities in UNSCR 1267. It is important to note in this respect that there is a mismatch between the time in which the sanctions committee issues/ updates the terrorist list and when EU regulations reflecting these updates are issued. Freezing measure therefore cannot be deemed to be taken "without delay" as per criterion III.1 of SRIII. Nonetheless, the evaluation team was informed that the Al-Qaida and Taliban Sanctions Committee notifies the Permanent Representation of Estonia to the UN of the amendments to the sanctions list and that the Ministry

of Foreign Affairs immediately forwards such notification to the FIU, the FSA and the Police and Border Guard. Nevertheless, since the European Commission takes a certain amount of time to update Regulation 881/2002 after the UN Security Council Committee lists a person, entity or organization, due to the procedural and translation requirements, the obligation in Estonia to freeze terrorist funds without delay is questionable. The evaluators note that under the ISA Act, no prior notice is given to the person who is the subject of an international financial sanction. Such notice is given only after the measure has been taken.

234. The evaluation team also notes that under Art. 2 of Council Regulation 881/2002 as amended: *"All funds and economic resources belonging to, owned, held or controlled by a natural or legal person, entity, body or group listed in Annex I, shall be frozen"* and that *"No funds or economic resources shall be made available, directly or indirectly, to, or for the benefit of, natural or legal persons, entities, bodies or groups listed in Annex I"*. There is no obligation therefore 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[30].

*Freezing assets under S/Res/1373 (c.III.2)*

235. As indicated above, Estonia relies on the mechanism provided under Council Regulation No. 2580/2001 to implement its obligations under UNSCR 1373. While it does not have an autonomous list separate from that of the European Union, it could, in principle, adopt national implementing measures under Art. 7 of the ISA Act, thereby complementing it.

236. Under Regulation 2580/2001 "all funds, other financial assets and economic resources belonging to, or owned or held by, a natural or legal person, group or entity included in the list annexed to the Regulation shall be frozen". The freezing of assets becomes applicable in all EU member states as soon as the list is amended by the EU Council. The freezing therefore applies without prior notification.

237. The regulation however does not explicitly extend the freezing measures to funds or other assets derived or generated from property owned or controlled, directly or indirectly by persons who commit or attempt to commit terrorist acts or participates in or facilitates the commission of a terrorist act. Nevertheless, Regulation 2580/2001 should be read in conjunction with Art. 1(2) of Common Position 2001/931/CFSP, which specifies "that for the purposes of this common position, "persons, groups and entities involved in acts of terrorism' means persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; entities owned or controlled directly or indirectly by such persons; and persons, groups and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons, groups and entities." This definition is in accordance with that set out in Criterion III.2 of the Methodology.

EU internals

238. Before the entry into force of the Lisbon Treaty on 1 December 2009, the list of designated persons and entities under the EU framework for the implementation of UNSCR 1373 distinguished between two categories of persons listed in the annexes to the Common Positions: (1) persons and entities classified as "external to the EU" i.e. falling within the remit of the common foreign and security policy of the EU and therefore subject to the freezing measures under Regulation 2580/2001; and (2) persons and entities classified as "internal to the EU" which fell under the third pillar of the EU concerning police and judicial cooperation for criminal matters. EU internals were not subject to automatic freezing measures but only reinforced police and

[30] The Estonian authorities pointed out that Estonia as an EU member cannot go beyond the requirements of the EU Regulation.

judicial cooperation. The freezing measures with respect to EU internals remained a competence of the individual Member States.

239. Following the entry into force of the Lisbon Treaty, the list of designated persons, groups and entities was updated through Council Decision 2009/1004/CFSP, which was enacted on 22 December 2009. EU internals were removed completely from the list of designated persons, since Art. 34 of the Treaty on European Union, which provided the legal basis for police and judicial cooperation, ceased to have effect. Hence European organizations such as the *Basque Fatherland and Liberty* (E.T.A.), the *Real IRA* and the Greek *Revolutionary Organization 17 November* are now completely absent from the list attached to the Regulation. However, Art. 75 of the Lisbon Treaty now provides an express legal basis for EU institutions to introduce EU-wide freezing measures against EU internals. To date, this measure has not been implemented by the EU. Freezing of assets of persons, groups and entities that were formerly referred to as EU internals continues to fall within the competence of each individual Member State. The implementation of UNSCR 1373 is therefore inadequate at the EU level.

240. Although the Estonian authorities have reassured the delegation that freezing measures against EU internals can be ordered under Art. 1(1) and (2) in conjunction with Art.7 and 8 of the ISA, the evaluators note that this possibility has never been exploited.

*Freezing actions taken by other countries (c.III.3)*

241. As concerns actions initiated under the freezing mechanism of other jurisdictions, under Regulation 2580/2001 an EU member state may request the listing of a person or entity from a non-member state. States that are not members of the EU can also make proposals concerning the designation of persons, groups and entities, which may lead to a listing in accordance with Council Common Position 2001/931/CFSP and Council Regulation (EC) No 2580/2001. When a proposal is made by a third state, the criteria for listing in Art. 1 of Common Position 2001/931/CFSP have to be fulfilled. Such requests must be examined by the EU Council, which must agree unanimously to act on the request.

242. If no such listing takes place, the Estonian authorities have informed the delegation that they could examine and give effect to the actions initiated under the freezing mechanism of other jurisdictions through the procedure provided under Art. 1(1) and (2) together with Art. 7 and 8 of the ISA.

243. Nevertheless, the provisions of ISA under Art. 1(1) and (2) together with Art. 7 and 8 only refer to international sanctions. ISA Art. 3 prescribes that international sanction means a measure which has been decided by the European Union, the United Nations, another international organisation or the Government of the Republic (of Estonia). These provisions do not explicitly:

a) state whether the Estonian Government is authorised to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions; and

b) provide for the procedures to be followed in cases where Estonia should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. Such procedures should ensure the prompt determination, according to applicable national legal principles, whether reasonable grounds or a reasonable basis exists to initiate a freezing action and the subsequent freezing of funds or other assets without delay

244. It was also noted that no examples of actions initiated under the freezing mechanism of other jurisdictions were provided by the authorities. The Estonian authorities stated that the Government of the Republic of Estonia may impose international sanctions and take relevant implementing measures under the ISA. So far, Estonia has only implemented the international sanctions and restrictive measures imposed by the UN and the EU. If an appropriate request is made to Estonia to

implement freezing mechanisms of other jurisdictions and no consensus is reached on the matter in the EU, then Estonia will consider the request and if it would be found reasonable and in accordance with the interests of Estonia, such measures could be imposed under the ISA. However, these provisions have not yet been tested in practice.

*Extension of c.III.3 to funds or assets controlled by designated persons (c.III.4)*

245. As indicated above, whereas EC regulation 2580/2001, together with Council Common Position 2001/931/CFSP provide for a freezing action which is in line with UNSCR 1373, EC regulation 881/2002 as amended does not extend the freezing actions to funds derived from funds or other assets owned or controlled, directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organizations.

246. The freezing action provided for under Art.4 of the ISA act, extends to "objects" in respect of which there is common or joint ownership between a number of persons of whom at least one is subject to an international financial sanction. It would be preferable, however, to align more closely the wording with criterion III.4 of SR.III, which requires that the freezing action should extend to funds or assets wholly or jointly owned or controlled, directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organizations.

*Communication to the financial sector (c.III.5)*

247. Under Criterion III.5, countries should have effective laws and systems for communicating actions taken under the freezing mechanisms to the financial sector immediately upon taking such actions. Under Art. 18 of the ISA Act as amended, the FIU must "publish information on the imposition, amendment or termination of international financial sanction immediately after receiving the information or must make it available on its webpage". Furthermore, under Art.13 (2) of the same act, obligated entities must consult regularly the FIU website for updates on international financial sanctions. Nonetheless, the authorities informed the delegation that updates on the sanction lists are sent regularly to obliged entities. This was confirmed by a number of banks and investment service companies, whereas insurance companies informed the delegation that they received such updates from the FSA, their supervisory authority. Some banks, however, highlighted that they downloaded the lists from the website of the European Union or consulted directly the OFAC list.

*Guidance to financial institutions and other persons or entities (c. III.6)*

248. In relation to the obligation to provide clear guidance to financial institutions/other person or entities that may be holding targeted funds/other assets concerning their obligation on taking action under freezing mechanisms, as already mentioned in this section, the ISA spells out such obligations. While this is considered a welcome development, the evaluators note that the lacunae identified in relation to criteria III.7 to III.9 also has a bearing on the fulfilment of criteria III.6.

249. The Estonian FSA has also issued advisory guidelines to explain legislation regulating the activities of the financial sector, and to provide guidance to subjects of financial supervision. The FIU has also issued new Advisory Guidelines of the Financial Intelligence Unit Regarding the Characteristics of Transactions Suspected of Terrorist financing on 21 January 2013 which identifies general indicators for suspicious transactions in relation to terrorist financing as well as activity indicators. Furthermore, it specifies that: credit and financial institutions and other subjects are required by law to verify upon the establishment of customer relationships and execution of transactions whether the natural person, legal person or other entity has been included in the Consolidated List of financial sanctions of the European Union or UN; and if a natural person, legal person or other entity included in the list has been detected, such institutions should notify the FIU promptly pursuant to subsections 32(1) and (5) of the MLTFPA and suspend the transaction. It is also noteworthy that under the ISA and Art. 29 of the MLTFPA obliged entities must set-up rules of procedures for the implementation of international financial sanctions and a

procedure to supervise its implementation. All FIU guidelines are available online on FIU webpage and are discussed within the Advisory Committee of Market Participants as well in Banking Association AML working group.

250. As Estonian authorities indicated, the FIU is in the process of adopting further guidelines for the reporting entities in order to provide added assistance in the implementation of SR.III related provisions.

*De-listing requests and unfreezing funds of de-listed persons (c.III.7)*

251. Formal de-listing procedures exist under the European Union mechanisms, both in relation to funds frozen under S/RES/1267 (1999) and S/RES/1373 (2001). Common Position 2001/931/CFSP of the European Union implementing S/RES 1373 (2001) provides for a regular review of the sanctions list which it has established. Moreover, listed individuals and entities are informed about the listing, its reasons and legal consequences. If the EU maintains the person or entity on its list, the latter can lodge an appeal before the General Court in order to contest the listing decision. De-listing from the EC Regulations may only be pursued before the EU courts.

252. As a member state of the EU Estonia relies on the formal de-listing procedures which exist under the European Union mechanisms, both in relation to funds frozen under UNSCR 1267 and UNSCR 1373. EU Regulation 881/002 provides that the Commission may amend the list of persons on the basis of a determination by the United Nations Security Council or the Sanctions Committee (Art. 7). EU Regulation 2580/2001 provides that the competent authorities of each member state may grant specific authorizations to unfreeze funds after consultations with other member states and the Commission (Art. 6). In practice, therefore a person wishing to have funds unfrozen in Estonia would have to take the matter up with the Estonian competent authorities who, if satisfied, would take the case up with the Commission and/or the United Nations.

253. Although the authorities in the third round had acknowledged that publicly known procedures for de-listing were not provided for under the law and needed to be addressed in the new ISA Act, the law as amended has not filled this lacuna. Authorities indicated that a person with regard to whom the measures provided in the act on the imposition or implementation of international financial sanction have been taken has the right to request the Financial Intelligence Unit to verify immediately if the measures have been taken lawfully. This includes dealing with de-listing request (in cooperation with other relevant authorities) and determining whether the person subject to asset freeze is a designated person. Furthermore, the authorities pointed out that it is common knowledge that unlawful acts of state authorities can be contested in administrative proceedings. The authorities have informed the delegation that should a person contact the FIU in this respect, the person would be guided on the procedure to be followed; they did not clarify however, what the procedure would consist of. Guidelines in this respect were to be issued in early 2014, however they still are outstanding.

254. The authorities also indicated that according to Art. 4(2) of the ISA, the provisions of the Administrative Procedure Act apply to the administrative procedures prescribed in the ISA, taking account the specifications provided for in the ISA. Implementing an international financial sanction is an administrative procedure. According to Art. 71(1) of the Administrative Procedure Act, a person who finds that his or her rights are violated or his or her freedoms are restricted by an administrative act or in the course of administrative proceedings may file a challenge. According to Art. 72(1) 1)-2) of the Administrative Procedure Act, the following may be applied for by way of challenge proceedings: repeal of an administrative act; repeal of a part of an administrative act unless partial challenge of the administrative act is restricted by law. According to Art. 87(1) of the same act, a person whose challenge is dismissed or whose rights are violated in challenge proceedings has the right to file an appeal with an administrative court under the conditions and pursuant to the procedure provided by the Code of Administrative Court Procedure. The Estonian

legislation, therefore, regulates the de-listing procedure. As the Estonian administrative procedure is regulated to sufficient detail, it can be said that de-listing is transparent and the rights of the individuals are protected.

255. Concerning the obligations regarding unfreezing the funds or other assets of de-listed persons or entities in a timely manner consistent with international obligations, some reporting entities (banks, notaries public, organisers of games of chance, Central Register of Securities) indicated that they would unfreeze funds if the FIU instructs them to do so, therefore it may be concluded that the unfreezing of the funds is not related to the fact that the person is de-listed, but the fact that FIU instructed reporting entity to do so. During the on-site, some reporting entities (investment funds and asset management funds, accountants, auditors) did not display knowledge of the obligation to unfreeze funds in a timely manner.

*Unfreezing procedures of funds of persons inadvertently affected by freezing mechanisms (c.III.8)*

256. Essential criterion III.8 requires that countries have effective and publicly-known procedures for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person.

257. As indicated above, under the ISA act as amended, obligated entities who have taken measures to implement a financial sanction must inform the FIU (Art. 12 and Art. 14 (2)). The FIU must thereafter verify, inter alia, whether: the measures taken are lawful; and if the person subject to asset freeze is a designated person and communicate the results to the notifying entity. Under the ISA act, a person subject to asset freeze may also request the FIU to determine whether the measures taken are lawful (Art. 19 of the ISA). The ISA does not explicitly specify what further actions and timeline the obliged entity must undertake and respect following the communication of the results of the verification by the FIU in either case: when the person does not result to be a designated entity, or, alternatively, when it is. From the interviews held emerged that, whereas credit institutions would unfreeze funds subject to a communication from the FIU in this respect, both the insurance sector and the DNFBPs were not aware of the procedure that would be applicable. Evaluators deem that additional clarity with respect to the procedure to be followed would be warranted.

*Access to frozen funds for expenses and other purposes (c.III.9)*

258. As concerns procedures for authorising access to funds or other assets which have been frozen pursuant to S/RES/1267(1999) and that have been determined to be necessary for basic expenses, Art. 2a of Regulation (EC) No. 881/2002 of 27 May 2002, provides the legal basis for unfreezing them subject to certain requirements. Notably, following a request made by an interested natural or legal person, the member State must satisfy itself that that funds or assets are (i) necessary for basic expenses, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges; (ii) intended exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services; (iii) intended exclusively for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources; or (iv) necessary for extraordinary expenses. Once this has been assessed, the determination must be notified to the Sanctions Committee. Exemption is granted if, in the case of use of funds established by virtue of points (i), (ii) or (iii), the Sanctions Committee has not taken a decision to the contrary by the end of the mandatory period of three working days, or, in the case of use of funds on the grounds of point (iv), if the Sanctions Committee has approved this use.

259. The authorities have indicated that the FIU is the competent body to authorize the release of funds in the above-mentioned cases. Under Art. 18 of the ISA, once the FIU has applied an international financial sanction, it must promptly inform the designated person, inter alia, of the

basis and procedure to benefit from an exception. The rapporteur deems that this would encompass access to funds or other assets which are necessary for basic expenses.

260. Any person wishing to benefit from these provisions must send their request to the relevant competent authority of the Member State listed in Annex II of the Regulation. The latter must notify the person having presented the request in writing, as well as any other person, entity or body recognised as being directly concerned, if the request is granted. The competent authority also informs the other member states of whether or not the derogation has been granted.

*Review of freezing decisions (c.III.10)*

261. The authorities have indicated that any person who feels aggrieved by a decision whereby his funds or other assets have been attached or frozen may apply to the court for redress. According to Art. 21 (5) of the ISA a complaint on the administrative act issued by the Financial Intelligence Unit or a proceeding carried out shall be filed with the administrative court. Thus the provisions of the Code of Administrative Court Procedure of Estonia apply to such procedure**.**

262. Freezing mechanisms envisaged by the relevant EU regulations can also be challenged at the Courts of the European Union. Natural or legal persons directly affected by a restrictive regulation or decision can challenge it under the general principle established by Art. 263 of the Treaty on the Functioning of the European Union. The legality of the freezing measure can also be challenged by bona fide third parties before the Courts of the European Union. Persons dissatisfied without actions taken to freeze their assets or funds can also lodge an application before the European Court of Human Rights.

*Freezing, seizing and confiscation in other circumstances (applying c.3.1-3.4 and 3.6 in R.3, c.III.11)*

263. The legislative measures described under Recommendation 3 are of general application and therefore apply to terrorist-related funds or other assets in the contexts other than those described in criteria III.1 – III.10. The deficiencies identified with respect to those measures also have an impact on compliance with criterion III.11.

264. In responses to questionnaire, Estonian authorities stated that the general criminal law framework and mechanisms on seizure and confiscation constitute to a large extent the basis for measures under SR.III, pending the adoption of a general new law on the application of international CFT sanctions.

*Protection of rights of third parties (c.III.12)*

265. As concerns the protection of bona fide third parties, according to Art. 6 of Council Regulation (EC) No 881/2002, "the freezing of funds, other financial assets and economic resources, in good faith that such action is in accordance with this Regulation, shall not involve the natural or legal person, group or entity implementing it, or its directors or employees, in liability of any kind unless it is proved that the freezing was due to negligence". Nonetheless, the Estonian authorities have advised that bona fide third parties may use the available civil remedies under Estonian law, including those for damages, if they feel aggrieved by any measure taken.

*Enforcing obligations under SR.III (c.III.13)*

266. Criterion III.13 requires that countries have appropriate measures to monitor effectively the compliance with legislation (…) governing the obligations related to SR.III and to impose sanctions if these are not complied with. Under Art. 20 and 21 of the ISA, the FIU exercises supervision over the implementation of international financial sanctions unless otherwise provided by law or the act of the European Union. Notably, it may: 1) verify whether obligated entities have set-up and apply the procedural rules as per Art. 13 of the ISA and verify their application; 2) carry out on-site inspections of the obligated entities; 3) issue precepts in order to receive information, including accounting documents from the obligated entities; 4) issue precepts in

relation to breaches of the obligations under the ISA[31]. Should the obligated entity fail to comply with the precept, the supervisory authority may apply a coercive measure under the Substitutive Enforcement and Penalty Payment Act of up to 1,300 euros, and 5,200 euros for subsequent breaches. The administrative act issued by the FIU and may be appealed before an administrative court.

267. Furthermore, under Art. 22 of the ISA, breach of the obligation to notify the FIU when a subject of an international financial sanction has been identified and to take measures provided under the ISA or the submission of false information is punishable by a penalty fine of up to 200 penalty units or an arrest. If committed by a legal person, the same act is punishable by a penalty fine of up to 20,000 euros. Under Art. 23 of the ISA, failure to set-up procedural rules to implement the obligations under the ISA is punishable by a penalty fine of up to 100 penalty units and by a penalty fine of up to 13,000 euros if committed by a legal person.

268. Furthermore under Art. 931 of the Penal Code, a person who knowingly performs acts or transactions with a subject of an international sanction or knowingly fails to apply other international sanctions is punished by a pecuniary punishment or up to 5 years' imprisonment. The same act, if committed by a legal person, is punishable by a pecuniary punishment. (3) The court shall also confiscate the object which was the direct object of the commission of the offence. Whereas the legislative framework in place seems to fully satisfy the requirements under criterion III.13, the rapporteur notes that certain effectiveness issues must also be borne in mind (see the relevant sub-section).

269. The FIU is responsible for supervising compliance with Special Recommendation III and has conducted relevant supervision in 2007 to 5 banks, in 2010 to 3 banks and in 2012 to 1 payment service provider. It is to be noted that the ISA entered into force in 2010. No breaches were identified and therefore no sanctions have been imposed on financial institutions or other reporting entities that failed.

270. Furthermore, in 2010 the FSA conducted an off-site examination of all credit institutions and branches of foreign credit institutions in order to assess the implemented transactions monitoring mechanisms. The scope of the examination also included an assessment of the procedures related to freezing of funds or assets of persons designated by the EU and UN Resolutions. According to the results of the assessment the transaction on-line and suspicious based monitoring mechanisms as well as the determination and freezing of the terrorist funds and the procedures of the treatment of related information were rated appropriate. No information on sanctions imposed were provided to evaluators**.**

*Additional element – Implementation of measures in Best Practices Paper for SR.III (c.III.14) and Implementation of procedures to access frozen funds (c.III.15)*

271. Although some aspects of the Best Practices Paper on the Freezing of Terrorist Assets are reflected in Estonian legislation (such as, for instance, notice of designation to the designated individual or entity), certain important elements of the freezing regime such as publicly known procedures for de-listing have not been implemented.

***Recommendation 32 (terrorist financing freezing data)***

272. Data concerning the number of persons or entities and the amounts of property frozen pursuant to or under UN Resolutions relating to terrorist financing is kept by the Estonian Internal Security

[31] During the on-site inspection the FIU may: 1) examine without limitations the relevant documents make excerpts, transcripts and copies thereof, receive explanations thereabout from the person to be examined, from the representative and employees thereof and monitor work processes; 2) receive explanations orally and in writing from the person to be examined, the representative and employees thereof. (3) The results of the inspection shall be recorded in the procedure provided for in Art. 50 of the MLTFPA.

Service and the FIU. The authorities have informed the delegation that no assets have been frozen as a result of measures taken under UN resolutions but that there have been freezing actions in relation to transactions related to suspicion of terrorist financing. However FIU has frozen assets linked to suspicious terrorism financing and in relation to EU regulations which are often in connection with UN resolutions**.**

***Effectiveness and efficiency***

273. The delegation notes that steps have been taken both at a legislative level and in practice to communicate in a more effective manner actions taken under the freezing mechanisms to the financial sector. Indeed updates on the sanction lists are sent to the obliged entities though this is not required by Estonian law. Estonian authorities consider that the most effective and prompt way to inform subjects via special e-mail lists and newsfeed in webpage: Search in designated persons lists (UN and EU): http://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing.dot; Changes in Al-Qaida and Taliban and related persons: http://www.politsei.ee/et/organisatsioon/rahapesu/rahvusvahelised-finantssanktsioonid/ Newsfeed about financial sanctions: http://www.politsei.ee/et/organisatsioon/rahapesu/el-i-ja-fatf-i-piiravad-meetmed.dot.

274. Credit institutions confirmed that they had internal written procedures on the freezing of terrorist assets. They were however unclear as to the exact procedure foreseen under the law in this respect. Doubts were expressed in particular as to the ability to freeze terrorist assets without the prior approval of the FIU. One credit institution in particular stated that without the approval of the FIU they could block a transaction but not the funds of a client. The delegation notes that this lack of clarity could hamper the promptness with which assets are frozen. However, all FIU guidelines are made publicly available on FIU`s homepage according to MLTFPA Art. 39(4) and further explained and introduced in Advisory Committee of Market Participants and Banking Association AML working group upon their establishment. Please see: https://www.politsei.ee/et/organisatsioon/rahapesu/juhendid/.

275. Some of the categories of reporting entities met on the occasion of the on-site visit did not seem to be very clear on the obligations deriving from the legal provisions implementing the UNSCR resolutions, or the manner in which the lists could be consulted. Not all the reporting entities had instruments to verify all their clients against the lists in a timely manner.

276. The FIU informed the delegation that in addition to the UN and EU terrorist lists there are no additional lists in Estonia.

277. Concerning supervisions, FIU has carried out supervision on international sanctions in 2010: 3 banks and 2012: 1 payment service provider. Furthermore FSA has also carried out the off-site supervision regarding implementation of international sanctions. Taking into consideration number of reporting entities and level of development of financial sector in Estonia, this number seems to be very low.

### 2.4.2 Recommendations and comments

***Special Recommendation III***

278. The enactment of the new ISA setting out the general legal framework for the application, implementation and supervision of international sanctions and thereby complementing in some respects EC legislation is a welcome development. Nonetheless some aspects require some additional measures to be taken.

279. Domestic legislation should address the shortcoming under Art. 2 of Council Regulation 881/2002 as amended, which does not encompass the obligation 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 as per criterion II.2 of SR.III.

280. The Estonian authorities should fully exploit the new mechanism enacted under Art.1(1) and (2) in conjunction with Art.7 and 8 of the ISA to take freezing measures against persons formerly known as EU internals. The authorities should also consider specifying the conditions which would need to be met to initiate a freezing action upon the request of a third State.

281. The authorities should consider aligning the wording of Art.4 of the ISA act with criterion III.4 of SRIII, which requires that the freezing action should extend to funds or assets wholly or jointly owned or controlled, directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organizations.

282. As concerns the obligations in respect of persons inadvertently affected by a freezing action, the ISA should specify what further actions the obliged entity must undertake and the timeline that must be respected, following the communication of the results of the verification by the FIU: when the person does not result to be a designated entity.

283. Although the legislative framework for monitoring the obligations which stem from the ISA is sound, the authorities should ensure that such supervision, including on-site inspections, are indeed carried out.

284. Authorities should consider enhancing the capacities of the FIU in respect of monitoring the obligations which stem from the ISA.

### 2.4.3 Compliance with Special Recommendation III

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **SR.III** | **PC** | • The requirement to apply freezing measures under UNSCR 1267 and 1373 without delay is not met;<br>• There is no 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;<br>• No measures have been taken to freeze funds of persons formerly known as "EU internals";<br>• No legislative framework to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions;<br>• No clear publicly-known procedures for un-freezing in a timely manner funds and assets;<br>**Effectiveness**<br>• Lack of awareness of SR III obligations by some reporting entities;<br>• Low number of supervisory visits in relation to the implementation of international financial sanctions and no sanctions have been imposed. |

***Authorities***

## 2.5. The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and analysis

***Recommendation 26 (rated C in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

285. The Estonian FIU was found fully compliant with rec. 26 and considered to be a generally effective FIU.

*Legal framework*

286. The Estonian FIU is a police unit, created on 1 July 1999 as a division of the Estonian Police Board. After becoming a section within the Central Criminal Police on 1 January 2004, it now finds its legal basis and statute in Chapter 4 of the MLTFP Act, making it structurally independent within the Police and Border Guard Board (MLTFPA Art. 36) since 18 January 2008. Beside the typical FIU functions it also has supervisory responsibilities over a defined number of FI and DNFBPs. It is no longer responsible for the ARB, as was the case at the time of the previous evaluation.

*Establishment of an FIU as national centre (c.26.1)*

287. The core functions of the FIU are laid down in Art. 37 MLTFPA. The FIU is the central and exclusive reception point of the information on suspected ML and FT activity as disclosed by the entities subjected to the reporting duty under Art. 32 of the Act. The disclosures take the form of suspicious transaction reports or currency transaction reports when related to an operation involving 32,000 euro or more or its equivalent in cash. It is in charge of processing and analysing such disclosures in order to identify potential money laundering and associated ("related") offences, and terrorist financing. When tracing and identifying "criminal proceeds" (Art. 37 (1) 3) it can take conservatory action to prevent dissipation of such assets. Foreign FIU requests and information are treated as SARs (Art. 46 MLTFPA and Art. 4(2) MoI Regulation 13 of 23/1/2008)

288. Besides dealing with SARs and CTRs, it also processes information related to ML/TF suspicions received from various state authorities and investigative bodies, which may eventually require (police) investigative action. According to the authorities the legal basis to pursue such information other than STR/CTR from the reporting entities is found in Art. 37(1)6) and Art. 37(2) MLTFPA, with art. 4(2) of the MoI Regulation no. 13 equating such communication with an STR.

289. Beside these core functions the FIU is also in charge of cooperating with reporting entities and investigative bodies (including foreign bodies) in ML and TF prevention, supervision over reporting entities, informing the public on prevention and identification of ML and TF, training of the reporting entities, as well as investigative bodies, prosecutors and judges in matters related to prevention of ML and TF, performing the tasks arising from the ISA, and of sanctioning of misdemeanours as provided for in the MLTFPA (Art. 37(1)).

290. The analysis of SARs runs through three stages. First the data clerk checks whether the report has been submitted in accordance with the regulations (Ministry regulation nr 51). Then the head of division or analyst performs a preliminary analysis of the disclosure based on available information from relevant databases, most of which are directly accessible to the FIU, so this process takes very little time. After confirmation of the suspicious character of the operation an analytical case-file is opened and enhanced analysis is undertaken (in-depth analysis and collection of all additional relevant data) which eventually may lead to the case being disseminated to the public prosecutor or investigation authorities.

*Guidance to financial institutions and other reporting parties on reporting STRs (c.26.2)*

291. Adequate guidance to the relevant entities on the manner of reporting is laid down in Art. 33 MLTFPA. Since 8 October 2010 disclosures, accompanied by any relevant document, must be made in a written form according to regulation No. 51 of the Minister of the Interior on "The Form and Instructions for Filling in Notifications Given to the Financial Intelligence Unit". This regulation contains guidance on the manner of reporting, specification of reporting forms and procedures to be followed when reporting. Any oral communication needs to be confirmed in writing.

*Access to information on timely basis by the FIU (c.26.3)*

292. Article 41 gives the FIU ample powers to query additional information complementing the disclosures for analytical purposes or to perform its functions in general, either on request (from other Authorities) or by "precept"[32] (from reporting entities). First of all it can "receive information from" all governmental or local authorities and the FSA, in order to "perform its legal functions" (Art. 41(1)), which is broader than complementing the STR/CTR disclosures to be processed. Secondly it can also obtain information from "surveillance" agencies, i.e. police and other law enforcement agencies conducting observations and intelligence gathering with the aim of detecting and preventing crime, with the proviso that they have to give their consent before the FIU can disseminate it further, but then only "in order to prevent money laundering" (art. 41(3)). .

293. Article 41(4) goes further by giving the FIU the "right" to request information from (unspecified) "third parties" if relevant for ML/TF prevention, including "accounting documents" in possession of any such third party that is somehow connected to the transactions under analysis. Basically this seems to give the FIU, in the performance of its analytical function, unrestricted access to relevant information that is in the hands of any person.

294. Different from the indirect procedure laid down in art. 41(1), Art. 42 MLTFPA gives the FIU the power to directly accede to state and local government databases and databases maintained by "persons in public law". In practice the FIU has direct access to some 34 d-bases (administrative and law enforcement) and indirectly to 2 customs related ones.

*Additional information from reporting parties (c.26.4)*

295. All entities subject to the reporting duty are obliged to supply any relevant additional information, including data protected by banking or other secrecy, at the request of the FIU within the deadline set by the FIU (art. 41(1) & (2). Non-compliance with such request or any administrative decision of the FIU can be sanctioned by the FIU (art. 38(4) MLTFPA). As a rule, this obligation applies to all entities subjected to the AML/CFT CDD rules, not only to the one that has reported. There is however one conspicuous exception: attorneys can only be queried about formal deficiencies in relation to their disclosures (Art. 41(5) MLPFTA). The authorities maintain that the attorneys, supported by their bar association, give a broad interpretation to this provision and that in practice they do give substantial additional information when requested.

296. The FIU uses these powers routinely, as shown in the table below:

**Table 14: FIU requests for information**

| | **Credit institutions** | **Other legal persons** | **Individuals** |
|---|---|---|---|
| 2009 | 4385 | 65 | 6 |

[32] Official translation. To be understood as "order".

| | | | |
|---|---|---|---|
| 2010 | 2615 | 103 | 10 |
| 2011 | 3236 | 103 | 11 |
| 2012 | 3316 | 63 | 1 |
| 2013 | 2549 | 57 | 9 |

*Dissemination of information (c.26.5)*

297. Whenever the analytical process produces sufficient added value and indications of money laundering or terrorism financing the relevant information, including whenever possible the probable predicate offence, is forwarded in a substantiated report to the appropriate law enforcement authorities (Art. 37(2), 43 (2) and (3) MLTFPA), *i.e.* the public prosecutor, the criminal police or the customs and tax board. Such dissemination is mandatory "upon detection of elements of a criminal offence", which is broader than the category of suspected offences (i.e. ML or TF) the subjected entities have to report according to Art. 32(1) MLTFPA and consequently may extend to predicate or other offences. The majority of the reports relate to suspected fraud. Beside the dissemination of FIU reports to the public prosecutor, information can also forwarded directly to other law enforcement authorities in simple cases whenever there are no sufficient grounds yet to initiate criminal proceedings (art. 43(3) MLTFPA). The significant number of FT related disclosures, mainly related to high risk territories, is sent without exception after a preliminary check to the Internal Security Service.

298. Besides at the initiative of the FIU, dissemination of FIU information is also possible when so formally requested by the law enforcement authorities (preliminary police investigation and prosecutors) and the court (Art. 43(3), when significant for the prevention, identification or investigation of money laundering, terrorist financing or related offence. In practice the FIU treats such requests as an STR. It goes further than supplying information from its d-base and also makes enquiries when prompted by such request.

299. The FIU can impose restrictions to the use of their information (in practice mostly "for intelligence purposes"). In no case the FIU report may contain any reference or personal detail of the individual that has submitted the SAR (43(5) MLTFPA). Finally the FIU may inform the FSA of any violation of the MLTFPA rules by a credit or financial institution (43(4) of the MLTFPA).

*Operational independence and autonomy (c.26.6)*

300. Although funded out of the general budget of the police, the FIU functions as a structurally and operationally independent department of the Central Criminal Police. This is explicitly laid down in Art. 36 (1).

301. The head of the Financial Intelligence Unit is appointed for a term of five years by the Director General of the Police and Border Guard Board on the proposal of the Deputy Director General in charge of the Criminal Police. The FIU cannot be subjected to an injunction from its hierarchy. Its IT system is stand-alone and only accessible to FIU staff. The funds allocated to them are deemed sufficient to enable it to perform its legal functions without constraints. The supervision of the FIU activities by the Data Protection Inspectorate on data processing and the Police and Border Guard Board on legality (art. 51 MLTFPA) does not affect its operational autonomy. No instances of undue interference have been reported as yet**.**

*Protection of information held by the FIU (c.26.7)*

302. The FIU operates under strict confidentiality rules. Dissemination of FIU information is only allowed in the specific circumstances as laid down by the law (Art. 43 MLTFPA – see above). As

said, only officials of the FIU have access to and may process the information registered in the FIU database (Art. 43(1) MLTFPA). All FIU staff has to maintain the confidentiality of the information that is known to them in their professional capacity, whether still active in the unit or not (art. 44(2) MLTFPA). The same confidentiality is imposed on the liaison officer of the Internal Security Service. There is however confidentiality and tipping-off risk involved when the FIU queries unregulated persons.

303. The database and computers of the FIU are protected by firewalls. The database of the FIU is kept on a separate server. The premises of the FIU are accessible only to the officials of the FIU. The entrance to the FIU premises is guarded by video cameras and an alarm system.

*Publication of periodic reports (c.26.8)*

304. Under Art. 37(1) and (5) the FIU is expected to inform the public on matters pertaining to the prevention and identification of money laundering and terrorist financing, to provide and comment on the relevant statistics, and to publish an overview annually.

305. The Estonian FIU publishes an annual report since 2005. It contains information on legal amendments, statistical information about the FIU's activities, overview of national and international cooperation, court decisions, sanitized cases, typologies and existing and emerging ML trends. The annual reports are made publicly available on the FIU's web-page in Estonian and in English[33]

*Membership of Egmont Group & Egmont Principles of Exchange of Information among FIUs (c.26.9 & 26.10)*

306. The Estonian FIU is a member of the Egmont Group since June 2000. The Egmont Secure Web is one of the most important channels for international information exchange the FIU uses extensively. The information exchange is governed by the Egmont Principles for Information Exchange, with unrestricted exchange of information with counterpart FIUs, including bank information and police intelligence information. The Estonian FIU signed the Egmont Group Charter in July 2013.

***Recommendation 30 (FIU)***

*Adequacy of resources to FIU (c.30.1)*

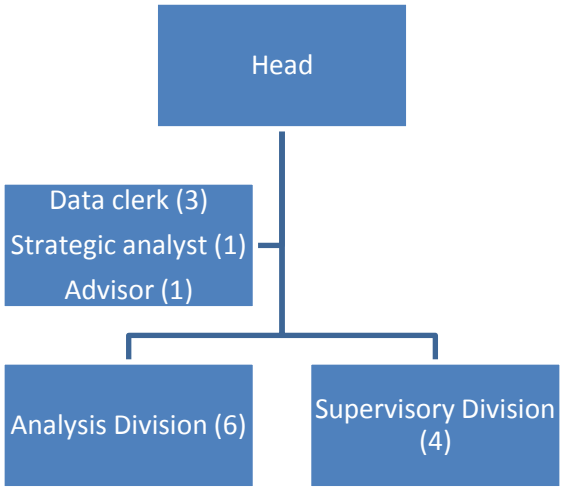
307. The FIU has its own permanent staff. Currently there are the following officials in the FIU: the head, 3 data clerks, one advisor and one strategic analyst. The FIU has 2 subunits: Analysis Division (6 officials), and Supervision Division (4 officials). The Analysis Division is responsible for analysing and disseminating SARs and CTRs. The Supervision Division is responsible for supervising the activities of obliged persons in complying with the MLTFPA. There is also a post of a strategic analyst under the Supervision Unit. The strategic analyst is responsible for gathering and analysing statistical data, ML trends and organizing feedback to reporting parties (annual reports of the FIU). At the moment of the on-site visit there was one vacancy. All in all the human resources are considered adequate.

308. Complementary to their main duties, the head of the FIU and the heads of the Analysis and Supervision divisions are actively engaged in providing the principal actors in the AML/CFT regime, such as the reporting parties, law enforcement agencies, prosecutors and judges with AML/CFT training.

[33]http://politsei.ee/et/organisatsioon/rahapesu/publikatsioonid/ http://politsei.ee/en/organisatsioon/rahapesu-andmeburoo/annual-reports-of-fiu/

309. The FIU does not decide on its own budget. It is dependent on the Central Criminal Police when it comes to budgetary issues, such as hiring staff, salaries and secondments to foreign countries. The technical resources of the FIU are deemed sufficient for an adequate functioning.

310. There have been some changes in the FIU staff since the third evaluation. The ARB is no more part of the FIU. It is separate bureau in the Central Criminal Police. Such decision was made to integrate asset recovery function more deeply with all criminal investigation units within the Police.




*Integrity of FIU authorities (c.30.2)*

311. Article 44(1) MLTFPA requires that the officials of the FIU must be of impeccable reputation, have the appropriate experience and abilities, and maintain high moral qualities before being appointed in the Unit. Officials of the Financial Intelligence Unit are required to maintain the confidentiality of information made known to them in the course of their official duties, including information subject to banking secrecy, even after the performance of their official duties or the termination of a service relationship connected with the processing or use of the information. The background of each candidate is checked thoroughly[34] and staff with access to data covered by state secrecy is subjected to an enhanced security and background check by the ISS.

*Training of FIU staff (c.30.3)*

312. The FIU staff is regularly provided with adequate and relevant training for combating ML and TF at both domestic and international level. During 2009-2012 FIU staff has participated in several training seminars. See Annex 4.

***Recommendation 32 (FIU)***

313. The FIU keeps comprehensive statistics on:

- the number of SARs received. This includes also the breakdown of the type of financial institutions or DNFBP or other business or persons filing the STR;
- the number of SARs analysed and disseminated. It should be noted that all SARs are analysed without exception. The FIU disseminated cases may aggregate several SARs.

[34] See also the Minister of Interior Regulation n° 15 of 12/4/2013,

314. The following statistics were supplied:

**Number of reports**

| | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|
| STR | 6263 | 5033 | 5988 | 6776 | 6637 |
| CTR | 10736 | 8622 | 7548 | 5381 | 4587 |
| Total | 16999 | 13655 | 13536 | 12157 | 11224 |

**Dissemination of reports**

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014[35] |
|---|---|---|---|---|---|---|
| Number of materials | 283 | 376 | 459 | 788 | 463 | 141 |
| Number of reports related to materials | 742 | 1118 | 1712 | 2087 | 1827 | 768 |
| For initiating criminal case (further investigation) | 39 | 55 | 83 | 47 | 17 | 25 |
| Initiated cases (initiated by the public prosecutor) | 29 | 47 | 77 | 41 | 12 | 17 |
| Initiated ML cases (initiated by the public prosecutor ML-specific) | 12 | 34 | 54 | 24 | 10 | 9 |
| Addition to existing investigation | 21 | 78 | 62 | 50 | 74 | 1 |
| As relevant information | 223 | 243 | 314 | 691 | 372 | 125 |
| Related amounts in million EUR | 2 560 | 450 | 255 | 281 | 2 560 | 95 |
| Number of related persons | 738 | 1127 | 1429 | 2109 | 1764 | 584 |

Disseminations of information by receiving entities:

| | 2013 | 2014 (5 months) |
|---|---|---|
| Tax and Customs Board | 229[36] | 52 |
| Internal Control of Police and Border Guard Board | 6 | 1 |
| Corruption Crime Bureau of Central Criminal Police | 5 | 11 |
| Criminal Intelligence Bureau of Central Criminal Police | 2 | 5 |
| Police Prefecture | 1 | 10 |
| Internal Security Service | 30 | 7 |

[35] (5 months)

[36] Most of these reports are handled administratively for taxation purposes and do not lead to prosecution.

| | | |
|---|---|---|
| LEA`s requests for criminal asset tracing | 46 | 18 |
| LEA`s requests for additional information answered | 52 | 21 |
| FSA | 1 | 0 |
| **Total number** | **372** | **125** |

**Predicate offences %**

| | 2012 | 2013 |
|---|---|---|
| E-fraud | 63 | 70 |
| Fraud | 25 | 20 |
| Drugs | 4 | |
| Tax Offences | 4 | 10 |
| Use of falsified document | 4 | |

**Prosecutions and convictions resulting from FIU reports:**

| | Sent applications to initiate criminal investigation | Not initiated | Cases closed | Convicted in court with Money laundering (PC Art. 394) | Convicted in court with other crimes | Still in phase of investigation (status of 24.04.2014) |
|---|---|---|---|---|---|---|
| 2010 | 55 | 3 | 29 | 5 | 6 | 12 |
| 2011 | 83 | 4 | 36 | 7 | 5 | 31 |
| 2012 | 47 | 2 | 21 | 3 | 0 | 21 |
| 2013 | 17 | 3 | 4 | 1 | 1 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| **For initiating criminal investigation (crime report to prosecutor):** | | **55** | **83** | **47** | **17** |
| * how many SAR were involved | | **84** | **127** | **69** | **27** |
| * how many CTR were involved | | **45** | **29** | **27** | **17** |

315. The police / prosecutor is obliged to inform the FIU about the status of the case: whether it was initiated or not; if initiated, on which grounds; if the case was sent to court or terminated; if it was sent to court, the FIU keeps track of the status of the case and the court judgment is added to the statistics.

316. FIU regularly monitors the status of the investigations based on the materials sent to the LEAs by the FIU (please see the table in Annex 3).

***Effectiveness and efficiency***

317. The 3rd round MER already came to the conclusion that the Estonian FIU operated in a good legal framework and adequately performed its central role in the Estonian AML/CFT system. This is presently broadly confirmed, some technical remarks aside.

318. The legal basis of the FIU as central reception point of the AML/CFT disclosures is solid, as is its framework governing the analytical and dissemination aspect. As for its analytical function, all in all the FIU has extensive powers of querying and obtaining (additional) information from

- all law enforcement agencies, including the Internal Security Service;
- the FSA;
- any entity subjected to the CDD rules;
- any administrative authority, such as any ministry, department, agency or other public authority;
- any other person, natural or legal.

319. There are however some issues that may be considered primarily technical, but not without possible impact on the performance of the FIU :

- The power of the FIU to query additional information from attorneys in circumstances where they are subjected to the reporting duty is severely restricted to incorrect or incomplete disclosures (Art. 41(5). The argument that this is broadly interpreted by the practitioners and the Bar Association does not offset the formal and restrictive legal provision which leaves no room for such flexible interpretation.
- The authority of the FIU to query any individual or legal person for additional relevant information is a powerful and useful tool, but also raises the question how the FIU can ensure the confidentiality of their request, as these persons are not bound to a tipping off prohibition or to any professional secrecy.

320. Looking at the statistical figures over the last 3 years on the output of the SARs & CTRs versus the input of the number of disclosures as a parameter of the level of effectiveness of the FIU, following conclusions can be made: disregarding the TF related reports (where the intervention of the FIU is minimal), the proportion varies from ca. 9% in 2010, over 13% in 2011 to 20% in 2012, indicating a substantial increase in terms of quantity. Some inference on quality can be made from the actual use of the outgoing analytical reports in investigations, showing a converse evolution: 159 out of 376 reports in 2010 (42%), 193 out of 459 reports in 2011 (42%) and 115 out of 788 reports in 2012 (14%). Although there are obviously a series of unknowns in this comparison, the figures show a distinct recent tendency of under-exploitation of the FIU material. The number of prosecutions initiated or supported by a FIU report, as ultimate effectiveness parameter, is still modest. The related statistics also raise questions.

321. Another point of attention raised by the statistics is the number of investigations pending since 2010: on a total of 202 reports sent to the PP, 76 are still under investigation (12 of them since appr. 4 years), or some 36%. Whilst the bare numbers obviously do not tell the whole story and the complexity of certain cases may require lengthy investigations, this delay appears also indicative

of an under-resourcing of the police and judiciary and/or an insufficient prioritisation of ML cases in the law enforcement effort

2.5.2 Recommendations and comments

***Recommendation 26***

322. The Estonian FIU is legally adequately resourced and takes up its responsibilities in a professional way. Looking at the impact of the FIU reports on the law enforcement results in terms of prosecutions and convictions, the picture is encouraging but not undividedly positive. The FIU reports are not being used optimally to trigger or support investigations and only occasionally lead to prosecutions and convictions. This is an effectiveness issue that should be addressed by the law enforcement community as a whole. Also there are still some formal legal issues that need to be addressed.

323. Therefore it is recommended that:

- the power of the FIU to query additional information from lawyers should be formally extended beyond the mere correction of incomplete or incorrect information (Art. 41(5) MLTFPA);
- legal measures be taken to safeguard the confidentiality of the FIU information when querying a non-regulated person, by inserting a confidentiality provision in the law, applicable to all person required to provide additional information at the request of the FIU;
- the causes for the under-exploitation of the FIU reports by the LE and judiciary authorities, and of the arrears in the ensuing investigations be examined and addressed.

***Recommendation 30***

324. The financial and human resources of the FIU are adequate and its staff complies with the standards of integrity and professionalism.

2.5.3 Compliance with Recommendation 26

| | Rating | Summary of factors relevant to s.2.5 underlying overall rating |
|---|---|---|
| **R.26** | **LC** | • Insufficient power to query all relevant additional information from lawyers;<br>• Confidentiality risk when querying unregulated persons. |

## 2.6. Cross Border Declaration or Disclosure (SR.IX)

2.6.1 Description and analysis

***Special Recommendation IX (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

325. The factors underlying the rating were the following:

- No designated authority to stop and restrain;
- No designated authority to seize;

- No comprehensive statistics yet available, making an effectiveness assessment impossible;
- Legislation does not cover transportation over EU borders.

*Legal framework*[37]

326. Since the 3rd round evaluation, Estonia designated the ETCB as the competent authority controlling the cross-border cash transportation by amending Art. 9 of Customs Act (2010), effective as of 1 May 2010, as follows:

*"(2) Upon controls of cash, the customs authorities shall apply the rules for customs control of goods. The definition "cash" is used in this Act within the meaning of Art. 2 (2) of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community*

*(3) For the performance of customs control and the establishment of circumstances, the customs authorities have the right to detain cash for up to 48 hours if a person has violated the obligation to declare cash provided for in Art. 3 of the Regulation of the European Parliament and of the Council specified in subsection (2) of this section, or if the customs authorities have reason to believe that cash is related to money laundering or terrorist financing*".

*Declaration system (c.IX.1)*

327. Estonia has adopted a declaration system of 10,000 EUR or more in cash or bearer negotiable instruments at its external EU-borders. According to Art. 2 of Regulation No. 24 of the Minister of Finance of 31 March 2010, any person arriving in Estonia from a non-Community state or travelling to a non-Community state from Estonia, carrying cash in an amount specified in Art. 3(1) of Regulation (EC) No. 1889/2005 of the European Parliament and Council of 26 October 2005 on controls of cash entering or leaving the Community (EUR 10,000), must submit a written cash declaration.

328. Regulation No. 24 defines "cash" by referring to Art. 2(2) of Regulation (EC) No. 1889/2005 of the European Parliament and Council, comprising all currency and bearer negotiable instruments. Control of the implementation of the cross-border cash transportation rules in Estonia are the responsibility of the ETCB, who monitor not only the physical transportation over the road, at the airport and the harbours, but also transportation by mail in the post office and by cargo. To that effect the ETCB have deployed staff at the post office and have issued internal regulations on the control of cargo at the airport and naval ports.

329. In practice the control is organised at the airport, the border crossing by railway, by road (3 posts) and at the naval ports. The ETCB also deploy mobile units. No equivalent or specific control

[37] MONEYVAL discussed the evaluation of SR IX in its EU Member States in the follow-up round during its 35th plenary meeting in April 2011. MONEYVAL noted that under the supranational approach, there is a pre-condition for a prior supranational assessment of relevant SR IX measures. It further noted that there is as yet no process or methodology for conducting such an assessment (although one is planned). Pending the FATF's 4th round, as an interim solution, MONEYVAL agreed that it will continue with full re-assessments of SR.IX in the 6 remaining EU countries to be evaluated (which includes Estonia). These countries will be evaluated using the non-supranational approach. Nevertheless, it noted that, for the purpose of Criterion IX.1, the EU has been recognised by the FATF as a supranational jurisdiction and therefore there is no obligation to comply with this criterion for intra-EU borders. Downgrading solely for the lack of a declaration/disclosure system is thus not appropriate. The other criteria that mention supranational approach (C.IX.4, C.IX.5, C.IX.7, C.IX.13 and C.IX.14) would not be evaluated against the requirements that apply to the supranational approach, and C.IX.15 would not be evaluated. The FATF was advised of this solution as it involves a departure from the language of the AML/CFT Methodology. At its plenary meeting in Mexico in June 2011 the FATF took note of this interim solution for EU Member States in MONEYVAL's follow-up round.

measures have been installed at the internal EU-borders. Any control there is done under the rules of the ETCB's general competence.

*In the case of discovery of a false declaration or absence of declaration, authority to request and obtain from the courier additional information concerning the origin of the funds or bearer negotiable instruments (c.IX.2)*

330. The cash declaration form must contain details of the origin and intended use of the cash. The ETCB control of goods rules are applied for the purpose of inspection of the cash declaration (Art. 9 (2) of the Customs Act). This includes verification of the correctness of the declared data and the right to request additional information and documents. Failure to declare and submit an incorrect or incomplete declaration is considered a misdemeanour pursuant Art. 91¹ of the Customs Act, which also gives the ETCB cause to investigate further.

*Power to stop or restrain currency or bearer negotiable instruments (c.IX.3)*

331. In case of non-declaration, submitting a false declaration, or suspicion of money laundering or terrorism financing cash is detained at the border for a maximum of 48 hours (Art. 9(3) Customs Act). In case of ML or TF suspicion the information is communicated to the Customs Investigation Department and to the Financial Intelligence Unit. In the case of a false or non-declaration a new, correct declaration must be submitted and misdemeanour proceedings are instituted. The cash is released whenever no grounds for seizure have been found (see also c.IX.10 and c.IX.11).

332. From the statistics supplied by the authorities, it appears that the temporary detention of cash is not a frequent occurrence, although the number is steadily increasing:

**Table 15: number of cases where cash was restrained**

| Year | Number of cases |
|---|---|
| 2013 | 8 |
| 2012 | 9 |
| 2011 | 8 |
| 2010 | 4 |
| 2009 | 5 |

*Maintaining collected information (c.IX.4) and Disclosure of information to the FIU (c.IX.5)*

333. The ETCB collect and register all information on cash declarations exceeding the threshold, together with the data on false or non-declarations. In case of suspicion of money laundering or terrorist financing the data are shared with the Financial Intelligence Unit who then initiates its own analysis and enquiries. Other law enforcement agencies (police, internal security service) have access to the ETCB's d-base on request.

334. There is no specific legal provision on the cooperation between the ETCB and the FIU, nor an obligation for the ETCB to directly inform the FIU of cash declaration matters or incidents. On the other hand the FIU does have access to all relevant information kept by the ETCB on the basis of Art. 41(1) MLTFPA. The present cooperative relations with the FIU are based on good practice and streamlined in an agreement with the FIU, specifying the grounds and conditions of exchange of information. In case of suspicion the FIU is informed immediately, otherwise the declaration data are communicated to the FIU twice a month.

*Coordination between the competent authorities (c.IX.6)*

335. The ETCB has mutual cooperation agreements with other state authorities, such as with the police and Internal Security Service. A procedure for exchange of information was agreed on 18.06.2010 between the Police and ETCB.

*Cooperation and mutual legal assistance at international level (c.IX.7)*

*336.* The ETCB is member of the World Customs Organisation and has customs assistance agreements with all the neighbouring states and many other states. On the basis of these agreements it is possible to exchange information about violation of customs rules and suspicion of violation. On the basis of Council Regulation (EC) No 515/97 of 13 March 1997, supervision information can be exchanged with the customs authorities of foreign states. The EU Regulation No. 1889/2005 establishes the grounds for exchanging other information concerning cash. The ETCB regularly exchanges information, including some cash related data, with its counterparts through its Customs Risk Management System. An agreement was concluded with the Russian Customs on bilateral exchange of declared cash data. The FIU in turn exchanges cash declaration information with foreign FIUs on case by case basis.

*Sanctions in case of false declaration (c.IX.8) and Sanctions in case of physical transportation of currency or bearer negotiable instruments in connection with terrorism financing or money laundering operation (c.IX.9)*

337. According to Art. $91^1$ of the Customs Act, failure to perform the obligation to declare cash, which has been stipulated in Parliament and Council Regulation No. 1889/2005/EC on controls of cash entering or leaving the Community is a misdemeanour punishable by a fine of up to 100 fine units (i.e. 400 EUR). It is applied by the ETCB on both natural and legal persons (in 2013 fines were imposed 7 times, and 1 in 2014) (Art. 73(2) of the Customs Act). In the event of ML or TF related cases discovered at the occasion of a cross-border cash transportation control the criminal code sanctions are applicable[38].

*Application of Recommendation 3 (c.IX.10) and Application of SR III (c.IX.11)*

*338.* Beside the possibility to detain cash for a period of up to 48 hours, undeclared cash cannot be seized solely on the basis of a declaration violation. In the event of notification to the FIU on grounds of ML/TF suspicions, the FIU can exercise its freezing powers. Seizure and confiscation measures are applicable whenever a suspicion of ML or TF warrants a criminal investigation and prosecution. In case of involvement of UN or other listed terrorists, the freezing mechanisms would also apply but this would normally trigger an intervention of the internal security service with seizure of the suspect cash. This has not occurred yet.

*Unusual cross-border transportation of gold, precious metals or precious stones (c.IX.12)*

*339.* If necessary, Estonian authorities can contact third countries and notify them or request additional information from them. Gold, precious stones, etc. can be viewed as goods and therefore the exchange of information falls under the customs assistance agreements. No such cases have been reported.

[38] Art. 391 of Penal Code, as amended on 1 February 2014, is now applicable: if the object of the act is a large quantity of goods or money (more than 32,000 Euros), the penalty, determined by the court, is a pecuniary punishment or up to three years' imprisonment. When it is a legal person, then the punishment will be one to five years in prison.

*Guidelines to the use of data (c.IX.13)*

*340.* As stated above, access to the ETCB d-base is purpose bound and restricted to law enforcement agencies and the FIU at their request. Reports to FIU are provided by accredited officials via encrypted e-mail. Reports about violations are shared with the Risk Management System IF, Customs Information System, Customs Enforcement Network and Customs Investigation Database FIDE according to security rules applicable to them.

*Training, data collection, enforcement and targeting programmes at a supra-national approach (c. IX.14)*

*341.* Training, data collection, enforcement and targeting programmes are developed and applied by ETCB. The authorities provided a list of training programmes provided to staff of the ETCB. The evaluation team consider the training provided to be adequate.

*Access to additional information at a supra-national approach (c.IX.15)*

342. This criterion is not evaluated within the context of MONEYVAL's 4th round, as indicated above.

*Additional element – implementation of the Best Practice Paper for SR.IX (c.IX.16)*

343. The authorities state they taken the best practices into account.

*Additional element – access to a computerised data base for AML/CFT purposes (c.IX.17)*

344. See comment Cr. IX 13

***Recommendation 30 (Customs authorities)***

345. The structure of the ETCB has not changed since the previous evaluation round.

346. All in all 294 customs offices are deployed at the borders at Tallinn Airport, in the naval ports, at highway border checkpoints (Narva, Koidula and Luhamaa) and railway border checkpoints (Narva and Koidula).

347. The Investigation Department of the ETCB, who also investigates tax related money laundering, is an independent unit reporting directly to the Director General of the ETCB and his or her Deputy. The unit has sufficient financial, human and technical resources to perform its duties adequately. According to Art. 30 of the CCP, the Prosecutor's Office directs pre-trial proceedings and ensures the legality and efficiency thereof and represent public prosecution in court.

348. In accordance with the Taxation Act (2002), Personal Data Protection Act, Public Information Act and other legal acts the ETCB has developed and implemented internal requirements for the protection of information. The Director General of the ETCB has issued an order on the "General Principles of Ethical Behaviour of ETCB Officials". This order is complemented by several guidance papers governing the integrity of officials and information protection.

349. The ETCB staff consists mainly of officials with Estonian Academy of Security Sciences education which provides skills and knowledge required for the job and who are reliable. Upon recruitment, special attention is paid to the reliability of the person, including background checks of the candidates.

350. One of the duties of the Customs Control is to secure the effective fight against illicit trafficking, related to ML/FT or not. Training related to the customs control focuses on securing the border control. Trainings for the customs control are planned yearly, including :

- base training for customs control
- examination of vehicles: cars, trucks, containers, etc.;

- drug-related training, incl. sniffer dogs and dog handlers;
- strategic goods controls, incl. dual-use goods and radiation controls;
- interrogation, conduct and conflict control;
- profiling and risk management.

351. All the officials of the border checkpoints are trained for effective customs control.

352. The officials of the ETCB have elementary knowledge of combating money laundering and terrorist financing obtained as part of their education in policing or law. The officials of the Investigation Department have not undergone special training in prevention of ML and FT and possible in-depth knowledge of the given area are based on self-education of the officials. However, some officials have undergone training related to proceeds of crime (seizure and confiscation of proceeds of crime

***Recommendation 32***

353. The authorities supplied the following statistics:

**Table 16: cash declarations**

| **Cash declarations on border from III quarter of 2007 to IV quarter of 2012** | | | | | | |
|---|---|---|---|---|---|---|
| Quarter | Total Number of Declarations | Amounts Declared (EUR) | Number of Export Declarations | Amounts Exported (EUR) | Number of Import Declarations | Amounts Imported (EUR) |
| 2007 III | 195 | 6,118,511 | 189 | 6,075,619 | 6 | 42,892 |
| 2007 IV | 245 | 9,851,694 | 233 | 9,694,629 | 12 | 157,065 |
| 2008 I | 189 | 11,048,151 | 181 | 11,037,132 | 8 | 11,019 |
| 2008 II | 164 | 4,571,738 | 155 | 4,463,133 | 9 | 108,605 |
| 2008 III | 283 | 8,331,900 | 277 | 8,323,524 | 6 | 8,376 |
| 2008 IV | 342 | 13,145,006 | 325 | 12,950,015 | 17 | 194,992 |
| 2009 I | 218 | 13,250,750 | 204 | 13,124,915 | 14 | 125,835 |
| 2009 II | 134 | 3,790,980 | 125 | 3,689,056 | 9 | 101,924 |
| 2009 III | 169 | 1,568,613 | 163 | 1,524,129 | 6 | 44,484 |
| 2009 IV | 268 | 5,770,417 | 268 | 5,647,953 | 19 | 122,464 |
| 2010 I | 296 | 77,610,720 | 288 | 77,293,852 | 8 | 316,868 |
| 2010 II | 231 | 4,162,812 | 211 | 3,724,628 | 20 | 438,184 |
| 2010 III | 278 | 9,559,514 | 237 | 6,597,830 | 41 | 2,961,683 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2010 IV | 304 | 13,068,259 | 253 | 10,313,514 | 51 | 2,754,745 |
| 2011 I | 403 | 83,033,129 | 370 | 73,982,753 | 33 | 9,050,376 |
| 2011 II | 363 | 57,468,956 | 337 | 54,245,243 | 26 | 3,223,713 |
| 2011 III | 390 | 114,512,348 | 357 | 108,393,848 | 33 | 6,118,500 |
| 2011 IV | 512 | 377,825,017 | 468 | 163,481,055 | 44 | 214,343,962 |
| 2012 I | 218 | 47,957,683 | 178 | 37,123,694 | 40 | 37,123,694 |
| 2012 II | 146 | 21,705,970 | 103 | 17,990,822 | 43 | 3,715,148 |
| 2012 III | 188 | 42,655,271 | 146 | 39,444,885 | 42 | 3,210,386 |
| 2012 IV | 255 | 42,422,628 | 208 | 40,419,702 | 47 | 2,002,926 |
| 2013 I | 267 | 34,397,546 | 222 | 32,687,767 | 45 | 1,709,779 |
| 2013 II | 278 | 35,342,316 | 227 | 32,780,312 | 51 | 2,562,005 |
| 2013 III | 332 | 49,350,904 | 274 | 46,123,794 | 58 | 3,227,110 |
| 2013 IV | 415 | 74,238,343 | 342 | 70,077,302 | 73 | 4,161,041 |

**Table 17: False declarations**

| Year | Cases | EUR (approximately) | Bases for detention |
|---|---|---|---|
| 2009 | 5 | 993 908 | False/incorrect declaration (cash not declared) |
| 2010 | 4 | 261 025 | False/incorrect declaration (cash not declared) |
| 2011 | 2 | 613 117 | Cash declared correctly but was detained in operation CASH (suspicion of criminal activity) |
| | 6 | 386 011 | False/incorrect declaration (cash not declared) |
| 2012 | 9 | 195 889 | False/incorrect declaration (cash not declared) |
| 2013 | 8 | 257 617 | False/incorrect declaration (cash not declared) |

**Table 18: notifications to the FIU**

| **Year** | **Suspicion not specified** | **Suspicion of ML** | **Suspicion of FT** | **CTR[1]** | **Total** |
|---|---|---|---|---|---|
| **2013** | 0 | 43 | 0 | 16 | 59 |
| **2012** | 25 | 6 | 0 | 10 | 41 |
| **2011** | 23 | 5 | 0 | 10 | 38 |
| **2010** | 16 | 1 | 0 | 6 | 23 |

[1] Notification of cash transactions which exceed the threshold.

| | | | | | |
|---|---|---|---|---|---|
| **2009** | 19 | 3 | 0 | 10 | 32 |

354. The majority of declarations are made by persons who are working for companies who offer payment services to their customers. The Estonian authorities initiated an investigation that resulted in the prosecution of a group of persons for ML (referred to under Recommendation 1). This ended up in an acquittal because the court did not accept the proof of the illicit origin of the money.

355. The Estonian FIU analysed the origin of the declared money and found that most of this money was transferred to Estonian banks from other EU country banks. The cross-border cash movements predominantly relate to accumulated savings and deposits from citizens of a neighbouring country in Estonian banks that are repatriated or used in commercial transactions. The risk is initially and primarily assessed by the banks under their CDD requirements. Estonian banks are quite popular with the citizens of a neighbouring country because of their professional and cheap customer service, compared to their local banks.

356. Although some of the information received from ETCB was included in FIU case files disseminated to the police, the authorities were not in a position to confirm whether any of these notifications triggered law enforcement action.

357. On cash related international exchange:

2009 - 1

2010 - 0

2011 - 4

2012 – 13

2013 - 27

358. As an example of good cooperation, the Estonian FIU and ETCB have undertaken a joint operation at Estonian borders in 2011 in order to identify possible violations of cash declaration system. During this operation the ETCB sent 8 STRs regarding cash declarations (on suspicion that the data declared was incorrect). In 2 cases the FIU used its freezing power, which was however lifted after verification.

***Effectiveness and efficiency***

359. Estonia has now fully integrated its cross-border cash transportation control regime in the Customs border control. The controls are focused on the traditional border crossing locations, but also adequately comprise in- and export of mail and cargo. Mobile units cover the areas with no fixed Customs border posts. Generally the statistics show a positive implementation picture.

360. From a technical point of view, there are some remarks to be made:

- From a technical point of view the FIU - ETCB interaction meets the requirements, the FIU having full access to the declaration information held by the ETCB. This right of access to the ETCB's information is purpose bound for SAR or CTR analysis (art. 41(1) MLTFPA). The information flow at the initiative of the ETCB to the FIU is not formally regulated, but is based on informal agreements (MOU) and best practices. Although this arrangement seems to function efficiently, it merits consideration to have it formalised in law.
- Particularly in comparison with other EU countries, the (maximum) range of sanctions is quite low, with little dissuasive impact, which also affects the enforcement effectiveness of the system.

361. Otherwise the statistics show a reasonable performance of the control regime. A typical feature of the Estonian system is the overwhelming dominance of outgoing declarations over ingoing, which is mostly explained because of the geographical position of Estonia as neighbouring Euro country to a non-EU country, the popularity of the Estonian banks as depository of assets of citizens from that country and the currency exchange facilities.

362. Although not a formal international requirement, in terms of effectiveness the lack of systematic international exchange of information is to be deplored. Neither the ETCB, nor the FIU make it a rule to inform their counterparts in all cases where the declaration involves a foreign citizen. The FIU does that only when they have to analyse reports from the ETCB on grounds of ML/TF suspicion, although the other threshold reports can also be very relevant and useful for the FIU of the involved traveller.

### 2.6.2 Recommendations and comments

***Special Recommendation IX***

363. Compared to the situation at the time of the 3d round MER Estonia addressed the main deficiency stated then by legally organising its border control for cash transportation according to the international standard and formally designating the ETCB as the competent authority to that purpose. The statistical figures indicate an acceptable level of implementation and control, particularly in the outgoing direction. Some aspects need closer attention, also from an effectiveness point of view:

- the authorities should consider to have the information flow to the FIU formally regulated, particularly in respect of the timely information of suspected ML or TF;
- the sanction range should be reviewed;
- there should be particular focus, both by the ETCB and the FIU, on systematic international exchange of operational information to the foreign counterparts on cross-border cash transportations by their nationals.

***Recommendation 30***

364. The ETCB is adequately resourced and trained. The recruitment of their officers is subject to an adequate integrity screening.

***Recommendation 32***

365. The ETCB keeps comprehensive statistics, although deplorably these do not give an indication of the ensuing LE results.

### 2.6.3 Compliance with Special Recommendation IX

| | Rating | Summary of factors relevant to s.2.7 underlying overall rating |
|---|---|---|
| **SR.IX** | **LC** | • Low sanctions. |

# 3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

***Legal framework and developments since third evaluation***

366. Since the adoption of the third mutual evaluation report in December 2008, Estonia has taken several legislative and regulatory measures in order to address the main deficiencies identified in the third evaluation round as well as to improve effectiveness. These developments are set out in detail under the description of each of the relevant recommendations.

***Scope of application***

367. The MLTFPA, which transposes the provisions of the 3rd AML/CFT Directive and its implementing Directive into Estonian Law, applies to all service providers in Estonia which engage in any one of the financial activities listed in the Glossary of definitions to the FATF methodology. As indicated in Table 4, all activities and operations referred to in the definition of financial institutions in the methodology, except for financial guarantees and commitments, are provided in Estonia.

368. The MLTFPA came into effect on 28 January 2008 and sets out the preventive measures applicable to operators in the Estonian financial and non-financial sector. Certain requirements in the MLTFPA only apply to credit and financial institutions[39].

369. The MLTFPA applies to credit institutions as defined under the CrIA. Art. 3(1) of CrIA provides that "*a credit institution is a company the principal and permanent economic activity of which is to receive cash deposits and other repayable funds from the public and to grant loans for its own account and provide other financing".* Branches of foreign credit institutions registered in the Estonian commercial register are also considered to be credit institutions for the purposes of the MLTFPA.

370. For the purposes of the MLTFPA, a financial institutions means:

*"1) a provider of currency exchange services;*

*2) a payment service provider within the meaning of the Payment Institutions and Electronic Money Institutions Act;*

*3) an electronic money institution within the meaning of the Payment Institutions and Electronic Money Institutions Act;*

*4) a provider of services of alternative means of payment;*

*5) an insurer engaged in life assurance within the meaning of the Insurance Activities Act;*

*6) an insurance broker engaged in mediation of life assurance within the meaning of the Insurance Activities Act (hereinafter insurance broker);*

*7) a management company and an investment fund established as a public limited company within the meaning of the Investment Funds Act;*

*8) an investment firm within the meaning of the Securities Market Act;*

*9) a savings and loan association within the meaning of the Savings and Loan Associations Act;*

*10) any other financial institution within the meaning of the Credit Institutions Act;*

[39] For instance, credit and financial institutions may exceptionally, at the request of the person participating in the transaction or the customer, enter into a business relationship before the full application of due diligence measures subject to certain conditions.

*11) a branch of a foreign service provider registered in the Estonian commercial register and providing a service specified in clauses 1)-10).”*

371. Article 6(2)10) refers to any other financial institutions includes the following: consumer credit providers, leasing companies.

372. The Payment Institutions and Electronic Money Institution Act entered into force in January 2010. This Act regulates “*the provision of payment services and e-money services, the activities and liability of payment institutions and e-money institutions and supervision over payment institutions and e-money institutions”*. Payment institutions and payment service providers are considered as ‘newcomers’ on the market. There were no e-money institutions licensed in Estonia at the time of the on-site visit.

373. As determined in Art. 6(4) of the MLTFPA a provider of services of alternative means of payment is a person who in its economic or professional activities and through a communication, transfer or clearing system buys, sells or mediates funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency, but who is not a person specified in subsection (1) or a financial institution for the purposes of the CrIA. Providers of services of alternative means of payment are required to be registered in the register of economic activities before commencing operations (Art. 52 of the MLTFPA). The evaluators were informed that the definition of “provider of services of alternative means of payment” has been set out in the MLTFPA to cover means of payment which are increasingly being performed in different electronic channels, which cannot be considered traditional methods of payment. New unconventional electronic payment systems are not usually account-based. A similar element of alternative systems is that they allow a party to a transaction to transfer money/value immediately, conveniently, securely and anonymously. The providers of alternative means of payment have been obligated persons since 2008. According to MLTFPA they have to apply all due diligence measures and other measures as financial institutions and other special requirements set out in Art. 15(8).

374. The MLTFPA contains a provision concerning the outsourcing of economic or professional activities of a financial institution to a third party. Article 28 provides that where such outsourcing is in place, the outsourced entity is deemed by law to be aware of the requirements under the MLTFPA. Outsourcing is subject to a number of conditions. Notably, the obligations arising from the MLTFPA should not be prejudiced, supervision should not be impeded and the outsourced entity has the required knowledge and skills to fulfil the requirements of the MLTFPA. Additionally, the financial institutions should be in a position to monitor performance of the AML/CFT requirements and the record-keeping requirements are fulfilled. Estonian authorities emphasised the fact that the outsourcing of economic or professional activities of a financial institution to a third party is based on the general principles and rules of Estonian legal system[40]. The explanatory notes to the MLTFPA state that the third party is considered to form part of the obligated person (performance aid). The obligated person outsourcing its activities is liable for infringement of the requirements of the MLTFPA.

375. The advisory guidelines “Outsourcing Requirements for Supervised Entities” were established by Resolution No. 84 of the Management Board of the FSA on 25 October 2006. Art. 6.2.3 of the FSA Advisory Guideline [41]stipulates that a supervised entity is required to inform the

[40]The public and private law are very clearly distinguished in Estonia. The principle of private autonomy is among the most fundamental principles of civil law and enjoys wide recognition in all aspects and dealings of both legal and natural persons. Therefore it is necessary to regulate the content of contracts between the obligated persons and their business partners, otherwise it would not be possible to ensure the adherence to the AML/CFT regulations in cases where the obligated persons have outsourced a part of their activities

[41] http://www.fi.ee/failid/EFSA_Guidelines_on_Outsourcing_Requirements_for_Supervised_Entities.pdf

FSA of outsourcing, since this is a material circumstance pertaining to the supervised entity's operations which may have a substantial impact on the interests of the supervised entity's customers. The notice to the FSA is accompanied with the relevant rules and procedures. According to the CrIA, Investment Funds Act, the Insurance Activities Act and the Payment Institutions and Electronic Money Institution Act, the service provider shall promptly notify the FSA of the transfer of operations and duties related to the economic and professional activities and submit a copy of the contract for transfer of operations. The relevant code of practice shall include a procedure for continued monitoring of the outsourcing risks. The FSA when assessing the rules may request the entity to make relevant changes in the rules of procedures to ensure that the necessary provisions are covered. When the financial institution does not meet the conditions of the request, the FSA has the right to issue a precept and prohibit certain activities (such as outsourcing) and require the termination of the transfer of activities or duties (based on sector acts and the Advisory guidelines of the FSA).

376. The evaluation team was informed that asset management companies outsource the issue and redemption of fund units and the maintenance of the register of the units to other service providers (usually credit institutions and the Estonian Central Register of Securities). In practice, they are therefore not in a position to apply AML measures themselves. The authorities deemed it necessary to regulate this situation by introducing Art. 28.

377. Asset management companies follow the FSA Guidelines (Advisory Guidelines) on the 'Outsourcing Requirements for Supervised Entities'. In doing so, they conduct a background assessment of the service providers, to ensure that the service provider is qualified to perform the relevant tasks and that the level of organisation and technical arrangements are adequate for the provision of the service. The adequacy of internal AML and CDD procedures of the outsourced entity is also determined. This is done by requesting information from the service provider and gathering information from third parties. The asset management companies monitor the service provider subsequently and assess the quality of the service annually.

378. In establishing the procedure for the monitoring of the service providers, the asset management companies have taken into consideration the fact that the unit-holder of the fund is always a customer of the credit institution or investment firm who carries out the customer due diligence. Therefore, the asset management companies have a reasonable expectation that in carrying out the CDD requirements, the service provider will follow the same procedure for its own clients. The asset management companies mainly focus on verifying that the standard the service provider uses is sufficient.

***Law, regulations and other enforceable means***

379. The AML/CFT preventive measures applicable to the financial sector are set out in the MLTFPA and relevant regulations of the Minister of Finance.

380. The MLTFPA empowers the Minister of Finance to issue secondary legislation to establish the criteria of low ML/FT risk for the application of simplified CDD measures and to set out detailed requirements for the rules of procedure to be implemented by credit and financial institutions. For this purpose, the Minister of Finance issued Regulations No. 10 and No. 11 on 3 April 2008 which entered into force on 11 April 2008.

381. The FSA has issued guidelines "*Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions*" ("FSA Guidelines") in October 2008 and has published it on its web-site. The document was last renewed in July 2013. One of the main purposes of the FSA Guidelines is to assist financial institutions in implementing and complying with their respective AML/CFT requirements, especially the risk-based approach. The FSA Guidelines specify how to implement the obligations stipulated in the MLTFPA, describe ML and FT techniques and provide examples for different risk factors.

***The definition of 'customer'***

382. In the MLTFPA different terms are used for a person entering into a business relationship, carrying out a transaction or otherwise requesting services from an obligated entity, as follows: (1) *a customer,* (2) *a person participating in a transaction,* (3) *a person participating in a professional operation, or* (4) *a person using a professional service.*

383. For the purposes of the MLTFPA, a *customer* is a person who enters into a business relationship with an obligated person. A *business relationship* is defined as a relationship of an obligated person, which: (1) in economic or professional activities is established upon conclusion of a continuing *contract* by the obligated person for provision of a service or sale of goods or for marketing goods otherwise; or (2) is not based on a continuing *contract,* but which may reasonably be expected to last for a certain term and during which the obligated person repeatedly makes independent transactions in the framework of their economic or professional activities, while providing a service or a professional service, performing professional operations or offering goods. The definition of a business relationship has been recently amended to ensure consistency of terminology used in different legal acts, most notably with the Notaries Act.

384. There is no definition of a person participating in a transaction, participating in a professional operation or using a professional service. Additionally, the use of such terms does not seem to be used consistently throughout the MLTFPA. At least sixteen articles have been identified in the MLTFPA where reference is made to one or more of these four categories. Of these, only 6 articles refer to all four categories of customer.

385. Estonian authorities stated that as a general rule, the use of one or more categories depends on the subject matter and scope of the specific provision and whether it applies to all of the obligated persons or is intended to apply to the conduct of a particular obligated person. Nevertheless, it was noted that certain basic requirements, such as the requirement to identify a customer under Art. 13(1) 1), only apply to a customer or a person participating in a transaction. Additionally, in the absence of a definition for the different categories of persons wishing to use the services of an obligated person (except for customer), it is unclear how obligated persons are expected to interpret these different provisions.

386. During the onsite visit financial institutions did not raise any difficulties as regards the usage of different terms of the person entering into a business relationship or carrying out a transaction. However, for the sake of clarity, it is recommended that the authorities review the MLTFPA to ensure that reference to a customer, a person participating in a transaction, a person participating in a professional operation, or a person using a professional service is used consistently.

The issue of "European and third country equivalence"

387. Under certain provisions of the MLTFPA (e.g. those relating to simplified CDD, reliance and permissible disclosures) EEA states are automatically presumed to have equivalent requirements to those under the MLTFPA. This presumption derives from the transposition by EEA states of European directives and regulations, which set out common and equivalent standards. It is to be noted that the FATF has not accepted the presumption that EEA states have equivalent AML/CFT frameworks. Therefore, systematically categorising all EEA states as adequately applying FATF standards is not appropriate.

388. With respect to countries outside the EEA, equivalence is assessed according to whether the third country applies requirements equal to those under the MLTFPA. It is the view of the evaluation team that the benchmark to be used by financial institutions to determine equivalence should be the FATF standards and not the MLTFPA.

389. In order to assist financial institutions in their determination of equivalence of third countries, the FSA issued a circular in 2009 to bring to the attention of financial institutions the

Common Understanding between the Member States on third countries equivalence (which was last updated on 26.06.2012)[42]. The list of equivalent countries was also published on the webpage of FSA[43] and on the webpage of FIU[44]. The circular letter indicates that despite the common understanding between member states, the obligated entity is still required to assess the risk while taking into account other risk indicators as well and to take measures to mitigate them. The circular refers to the fact that if a country does not appear in the list, it does not necessarily indicate the low-level standards of AML/CFT laws and due diligence measures and does not demand qualifying the country as non-equivalent. It should be noted that the FATF has in the past challenged the reliability of the EU list.

390. Based on the provisions of the FSA Guidelines it seems that the list of the equivalent third countries is only one indicator that assists obligated persons in determining the risk levels of a customer or person participating in a transaction. Additional circumstances also must be taken into consideration as well as other factors as determined in the FSA Guidelines.

391. Financial institutions in any case have an obligation to apply enhanced CDD measures in relation to non-equivalent countries based on Art. 14(5) of the MLTFPA. Financial institutions are required to pay special attention to business relations and transactions if the place of residence or seat of the customer, or the seat of the provider of the payment service of the beneficiary is in a third country or territory where AML/CFT measures have not been taken, the tax rate is low and which is not engaged in international cooperation (high risk countries).

***Customer Due Diligence and Record Keeping***

### 3.1. Risk of money laundering / financing of terrorism

Financial activity carried out on an occasional or very limited basis

392. Estonia has not exercised the option provided by the FATF Recommendations not to apply some or all of the AML/CFT measures to certain natural or legal persons carrying out a financial activity on an occasional or very limited basis (according to quantitative and absolute criteria), such that there is little risk of money laundering or financing of terrorism.

Modulation of preventive measures according to risk

393. Since the last mutual evaluation report, the MLTFPA, supplemented by the regulations of the Minister of Finance and the relevant guidelines issued by the FSA and the FIU, has further strengthened the concept of the risk-based approach to increase the effectiveness of the Estonian AML/CFT regime.

394. According to Art. 14(3) of the MLTFPA, an obligated person shall apply all the CDD measures as specified in subsection 13(1) of the MLTFPA, but may choose the appropriate scope of application of the CDD measures based on the risk level of the person participating in the transaction or professional operation. It is important to note that the application of the risk-based approach does not exempt financial institutions from any of the CDD requirements. According to Art. 14(3), all CDD measures are to be applied when establishing a business relationship or carry out an occasional transaction. However, the degree of application of the CDD measures can be calibrated according to the level of risk posed by the business relationship or a transaction.

[42] Common Understanding between Member States on third country equivalence under the Anti-Money Laundering Directive (Directive 2005/60/EC), available: http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf.

[43] http://www.fi.ee/index.php?id=3375

[44] http://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/riigid-kus-kehtivad-rahapesu-ja-terrorismi-rahastamise-samavaarsed-nouded.dot

395. Article 29(1) of the MLTFPA requires all obliged entities to have in place written rules of procedure for the application of CDD measures, including the assessment and management of the risk of ML and TF and the collection and preservation of data.

396. According to Art. 30 of the MLTFPA, all financial institutions must establish rules of procedure and appropriate internal controls. Regulation No. 10 stipulates that internal controls must correspond to the type, scope and complexity of the economic or professional activities of the financial institution and regulate, among others, the application of due diligence measures. The rules of procedure must describe transactions of a lower risk level as well as of a higher risk level and establish the appropriate requirements and procedure for entering into such transactions.

397. The FSA Guidelines specify how to implement risk based approach and provides different risk factors. CDD must be applied on a risk-sensitive basis. The nature of the business relationship or transaction and the risks arising therefrom must be taken into account when determining the extent of measures to be applied. Risk-based CDD calls for the prior weighing and mitigating of risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, normal, enhanced or simplified due diligence measures could be applied). The FSA Guidelines also clarify that in cases where the risk level of a customer or a person participating in a transaction is low, the obligated person may apply simplified due diligence measures, but is not allowed to do away with customer due diligence entirely. If the risk level arising from a customer or a person participating in a transaction is high, enhanced due diligence measures must be applied. The responsibility for the preparation of the required procedure lies on the financial institution.

398. The MLTFPA permits the application of simplified CDD measures, in the event of a low risk of ML and TF, but only in relation to several determined customers and products, based on the instances provided by the 3rd EU AML/CFT Directive and the implementing directive. Article 17(1) of the MLTFPA determines that upon fulfilment of the conditions provided for in Art. 18 of the MLTFPA, a financial institution may conduct simplified CDD determining the appropriate scope thereof pursuant to the nature and risk of the business relationship, the transaction or customer. If the financial institution decides to apply simplified customer identification it shall, at its own discretion, select the customer identification measures, as well as their scope. According to Art. 17(3) of the MLTFPA the financial institution must gather sufficient information to determine whether the transaction or customer qualifies for the application of simplified CDD. During the onsite visit the evaluators were informed that sufficient information must at least include the identification data referred to in Art. 23 and 24 of the MLTFPA.

399. Regulation No. 11 on the "*Criteria of low risk of money laundering and terrorist financing which allows the application of simplified customer due diligence measures*" is established on the basis of Art. 18(5) of the MLTFPA. The regulation sets out the criteria of low risk for persons participating in a transaction, customers and transactions. The regulation shall not be applied if it appears from publicly available information that the risk of ML and TF is not low related to a client or a transaction. Simplified CDD measures may only be applied where the financial institution clearly specifies the instances where this is permissible in its rules of procedure. Simplified CDD shall not be applied if there is a suspicion of ML and TF and the obligated person must be ready to apply CDD measures determined in Art. 13(1) of the MLTFPA.

400. Regulation No. 10 requires credit and financial institutions to describe the low risk transactions, and procedures of the conclusion and monitoring of such transactions. The FSA Guidelines provide that where the risk is low, the obligated person may apply simplified CDD measures however only on the conditions provided in Art. 18 of the MLTFPA, in accordance with the Minister of Finance Regulation No. 11 (depending on the decision of the obligated person on risk factors).

401. In order to assist financial institutions in their determination of equivalence of third countries, the FSA issued a circular in 2009 to bring to the attention of financial institutions the Common Understanding between the Member States on third countries equivalence (which was last updated on 26.06.2012).

402. The FSA Guidelines determine (point 4.6.7.3) that in a situation where at least one risk category or factor can be identified as high, the risk level of the customer or person cannot usually be low. Equally, the low risk does not necessarily mean that the customers operations cannot be associated with ML or TF at all.

403. *Enhanced CDD* is required by the MLTFPA if the nature of a situation involves a high risk of ML and TF. Article 19(1) of the MLTFPA stipulates that in higher risk cases, a financial institution shall apply enhanced CDD. Additional due diligence measures must be applied in the events of high risk transactions and situations, which are determined in Art. 19(3) of the MLTFPA. An obligated person shall apply at least one or more due diligence measures specified in subsection 19 (3) of the MLTFPA in addition to the measures provided for in Art. 13(1)1)-4). Financial institutions may decide on other risk factors as defined in the MLTFPA and are responsible for the proper application of due diligence measures.

404. Additionally, enhanced CDD is required by the MLTFPA for non-face-to-face business relationship, PEPs of other EU member states and third countries, cross-border correspondent banking relationship of third countries, and where there is doubt regarding the truthfulness of the data or authenticity of the documents submitted for identification and verification purposes. The first three risk-categories are modelled on the risk-based approach set out in the 3rd EU AML/CFT Directive and are not the result of a specific risk assessment of the Estonian financial sector.

405. Based on Regulation No. 10 financial institutions are required to apply enhanced CDD for high risk transactions, based on the risk factors which financial institutions have identified in their rules of procedures, including private banking transactions.

406. In addition to these categories, currency exchange services, payment services and services of alternative means of payment are considered to be higher risk categories and required to apply CDD measures for transactions with lower thresholds than 15,000 EUR. Special requirements are determined for the currency exchange services in the MLTFPA. Upon provision of currency exchange services, a provider of currency exchange services shall identify and verify all persons participating in the transaction if the amounts exchanged in cash either in a single transaction or related transactions exceed 6,400 euros or an equal amount in another currency. A provider of payment services shall identify all customers who make or receive money transfer.

407. According to the FSA Guidelines if the risk level arising from a customer or a person participating in a transaction is considered to be high, enhanced due diligence measures must be applied in accordance with Art. 19, 21 or 22 of the MLTFPA.

408. During interviews held on site, the authorities demonstrated awareness of the ML/FT threats in Estonia. Information obtained from threat assessments conducted at an institutional level (mainly FIU and FSA) highlights a number of higher risk areas in Estonia. Business conducted by financial institutions with customers from certain neighbouring countries is considered to pose one of the highest ML risks. In recent years, the obligated entities considered to be most vulnerable to ML have been payment services providers as "newcomers" on the market (including alternative payment services) and traders in precious metals. The FIU identified a number of ML schemes where funds obtained from cybercrime were transferred through the payment services market to 'straw men', withdrawn in cash and physically transported to neighbouring countries. Some traders in precious metals were found to have been involved in ML operations relating to proceeds generated by tax-fraud offences. The results of the institutional threat assessments also indicated that the widespread use of IT in Estonia could potentially increase the ML/FT risk within the

financial sector. However, the TF risk is considered to be low. Due to an increase in ML/FT risk associated with NPOs in the past few years, the Estonian authorities decided to extend the scope of the MLTFPA to the non-profit associations and foundations where a cash payment equal to or exceeding the amount of 15,000 euro is made. However, the terrorist threat level and the risk of terrorist financing remain low in Estonia[45].

409. The analyses of recent investigations indicate that new money laundering schemes that are used are those where payment service providers are used to transfer funds or to withdraw cash. According to the Estonian authorities the use of off-shore companies in ML schemes has decreased. Alternative e-money services like on-line gambling and virtual currencies (Linden Dollars, Second Life, Bitcoin) are also under highest attention, although no real ML cases have been detected. Estonian citizens, private and public companies as well as service providers have been keen to introduce and use different e-services (like mobile payments, e-banking, debit cards, etc.), so the authorities focus on potential risks and vulnerabilities that might originate from e-services as well.

410. Most financial institutions consider cash transactions, business originating from certain neighbouring countries, and tax havens as presenting higher risk of ML and TF.

411. A number of measures were implemented by the authorities to mitigate risk. The FSA and the FIU have assessed risks and vulnerabilities of the different sectors on a regular basis. The findings of the FIU were published in the annual reports in order to increase awareness. The FIU introduces ML trends regularly to the Governmental Committee. This information has been analysed in the national risk assessment project as well. The existing and emerging ML trends are described in its annual reports which are available in FIU website in Estonian and in English. It provides an overview of new money laundering schemes detected by the FIU and of court judgments on money laundering. The FSA has procedures in place for mitigating the risks of the financial sector.

412. The assessors were informed that the rules of procedure of financial institutions are monitored during inspections visits and the risk factors identified in the internal procedures are usually discussed with the FSA.

413. The FSA provided a model for risk assessment for financial institutions, which includes a method on how to determine the risk level when entering into business relationship or carrying out an occasional transaction. The model and the methodology have been explained to financial institutions in several training seminars. The model includes the assessment of the threats and vulnerabilities arising from the activities of financial institutions, as well as measures to detect threats and measuring the vulnerability of each threat. Four categories associated with the customer must be taken into account: place of residence or seat of the customer (country and geographical risks); parameters characterising the customer (customer risk); economic activities of the customer (product and service risk); and transaction partners of the customer and other related risks (risk of the transaction partners and the country and geographical risks, products risks).

Use of risk-based approach by the supervisory authorities

414. The FSA applies risk-based supervision. This includes regular monitoring of the activities and risk management systems of financial institutions, as well as conducting regular off-site controls in order to assess the implementation of the compliance measures and effectiveness of the risk

[45] In the view of the Estonian authorities. Also According to Europol's Terrorism Situation and Trend Report (2013), Estonia remained one of the least affected countries in Europe. According to Estonian Internal Security Service, there were no active terrorist groups in Estonia in 2012 or supporters or financiers of international terrorist organisations. Some fundamentalist Islamic organisations continue to show interest in furthering its activities both in Estonia and in neighbouring countries.

assessment models, i.e. the vulnerabilities that may affect the activities of financial institutions. The FSA analyses the vulnerabilities and threats associated with all financial institutions. According to the results of the analyses, the FSA draws up the plan of supervisory activities. The annual plan is subject to the approval of the management board of the FSA. In addition to the planed on-site examinations, the FSA conducts *ad hoc* supervision in order to assess and mitigate other unexpected risks.

415. Further information on the risk-based supervisory practices of the FSA is provided under Section 3.6 of this report.

The National Risk Assessment

416. In 2012, the Ministry of Finance initiated a National Risk Assessment (NRA) in order to identify, assess and take effective actions to mitigate AML/CTF risks regarding the financial as well as DNFBP sector. For that purpose Estonia used the methodology of the World Bank (World Bank Risk Assessment Methodology and its Second Generation Tool). The results of the NRA are expected to provide the basis for more focused approach to supervision and have therefore substantial influence to the risk-based approach applied in the supervisory activities. Additionally, the results of the NRA highlight the areas in which the legal norms could be further improved. Furthermore, the NRA provides grounds for the efficient allocation of resources across the AML/CFT regime and the implementation of relevant preventive measures.

417. In order to complete the NRA and introduce the Second Generation NRA Tool and distribute the work between the sub working groups, the Ministry of Finance in cooperation with the World Bank carried out a 2-day seminar on 25-26 February 2013 where over 60 representatives from different relevant institutions participated, including, the representatives from Ministry of Finance, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Justice, FIU, FSA, Estonian Internal Security Service, Police and Border Guard Board, Office of the Prosecutor General, ETCB, Advisory Committee, Estonian Banking Association, Estonian Chamber of Commerce and Industry, etc. During the seminar 5 sub-working groups were formed and the relevant work is conducted in those sub working groups under the supervision of Ministry of Finance of Estonia.

418. During the onsite visit, the evaluators were also informed on the ongoing process of the NRA. However, it was too early to discuss preliminary conclusions. In the 5 subgroups which have been set up, the work is ongoing on differentiated topics (criminal proceeds, national risks, financial sector, securities, DNFBPs), involving various experts. The authorities were at the time of the onsite visit in the process of drawing up preliminary conclusions and results. The coordination of the ongoing work is provided by the Ministry of Finance and the Governmental Committee.

419. The intended outcome of the NRA could highlight areas (in the financial or non-financial sector) in which the regulations could be further improved, or in which more awareness-raising, e.g. training is needed. Furthermore, it could provide the basis for more focused approach to supervision. The NRA was expected to be finalised during 2014 and in following years the NRA will be updated regularly. An Action Plan will be adopted as result of the NRA which will describe main actions which need to be taken to ensure that the current system of combating the money laundering and terrorism financing is more effective, including eliminating any weaknesses found.

## 3.2. Customer due diligence, including enhanced or reduced measures (R.5 to R.8)

3.2.1 Description and analysis

***Recommendation 5 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

420. As described in the 3rd round report, Estonia was rated "Largely Compliant" for Recommendation 5. A few minor deficiencies were identified in the legal framework: no guidance was provided on third countries considered to have adopted equal requirements to those of the MLTFPA, there was no clear requirement to identify a natural person acting on behalf of another natural person, no guidance was provided on the existing categories of enhanced CDD, and no requirement to terminate a business relationship when additional documents are not presented upon request.

421. The 3rd EU AML/CFT Directive was implemented in Estonia with the adoption of the MLTFPA in 2008 as reported in the MONEYVAL 3rd round MER. Since then, several amendments have been made to the MLTFPA, in order to address the deficiencies identified by the MONEYVAL evaluators and other issues identified by the Estonian authorities.

422. Minister of Finance Regulation No. 10 on "*Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance*" was published on 3 April 2008 and requires credit and financial institutions to describe low and high risk transactions, and procedures of the conclusion and ongoing monitoring of such transactions.

423. The FSA and the FIU have issued guidelines to assist credit and financial institutions in the implementation of their requirements, including the application of the risk-based approach.

*Anonymous accounts and accounts in fictitious names (c.5.1)*

424. The prohibition of anonymous accounts and accounts in fictitious names is implemented through a combination of provisions in the MLTFPA. Anonymous accounts are *expressis verbis* forbidden according to Art. 15(3) of the MLTFPA which states that credit and financial institutions "*shall not enter into a contract or make a decision on opening an anonymous account or savings bank book. A transaction in violation of the prohibition shall be void."*

425. Article 15(2) requires credit and financial institutions to open and keep an account only in the name of the account holder. As a result, accounts in fictitious names and numbered accounts are not permissible. Furthermore, Art. 15(2) does not permit credit and financial institutions to provide services that can be used without the identification (and verification of the identity) of the person participating in a transaction.

426. These requirements are reinforced by Art. 15(1) which states that when opening an account or providing a service outside of a business relationship for the first time, the credit or financial institution shall identify the prospective customer on a face-to-face basis.

427. As an overarching requirement, financial institutions are required to apply CDD measures when establishing a business relationship or carrying out an occasional transaction, including identifying the customer and verifying his identity (Art. 13(1)).

428. As determined in Art. 57 of the MLTFPA, opening an anonymous account or savings book or signing a corresponding contract on the part of an employee of a credit or financial institution is punishable by a fine of up to 300 fine units[46] (equivalent to EUR 1,200). In case of a legal person, the fine to be imposed may be up to 32,000 euros.

[46] According to Article 47 of the PC, a fine unit is the base amount of the fine and is equal to EUR 4.

429. Estonian authorities confirmed that anonymous, fictitious or numbered accounts have never been legal in Estonia. This was confirmed by reference to paragraph 96 of the 1st round MER, paragraph 190 of the 2nd round MER and paragraphs 454 and 499 of the 3rd round MER. The present and previous AML Laws expressly require that accounts can only be held in the name of the account holder.

***Customer due diligence***

*When CDD is required (c.5.2*)*

430. According to Art. 12(2) of the MLTFPA financial institutions shall apply CDD measures at least:

1) upon the establishment of a business relationship; (criterion 5.2(a))
2) upon entering into or mediating on an occasional basis transactions the value of which exceeds 15,000 euros or an equal amount in another currency, regardless of whether the financial obligation is performed in one payment or in several related payments[47]; (criteria 5.2(b))
3) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided by law; (criterion 5.2(d))
4) when the documents or data gathered earlier while identifying and verifying a person or while updating the respective data prove to be deficient or there is doubt about the veracity of the documents or data. (criterion 5.2(e))

431. Pursuant to Regulation (EC) No 1781/2006 of the European Parliament and Council on information on the payer accompanying transfers of funds (implementing SR VII), which is directly applicable in all EU member states, financial institutions in Estonia are required to register the transaction data and ensure that the required originator information is included in wire transfers (Art. 25 of the MLTFPA), where the transaction exceeds EUR 1,000.

432. As a general rule, upon entering into a business relationship with a credit or financial institution or upon the first use of a service, the potential customer or the person participating in the transaction must be physically present (Art. 15(1) MLTFPA)[48]. This goes beyond the FATF requirements.

433. Over and above the instances set out under Art. 12(2), Art. 15 provides for a series of additional specific circumstances within the context of payment services, currency exchange services and alternative means of payment, where certain CDD elements are required. These go beyond what is required under Recommendation 5. The authorities indicated that these provisions were introduced since the activities of payment services providers, currency exchange offices and alternative means of payment providers are considered to pose a higher risk and therefore necessitated the imposition of more stringent requirements.

434. According to Art. 15(7) of the MLTFPA, a payment services provider shall identify all customers who make or receive money transfers through the payment services provider. Payment service providers are therefore required to comply with identification requirements beyond the threshold of EUR 1,000 for wire transfers referred to under Regulation 1781/2006 and EUR 15,000 for other payments.

[47] Article 14(2) states that if a financial obligation is performed in a transaction by way of several related payments and the total amount of these payments is unknown, the person must be identified and verified as soon as the amount provided for in Article 12(2) 2) is exceeded and becomes evident.

[48] However Art. 15 of the MLTFPA provides for some exceptions to the rule.

435. The same applies to providers of alternative means of payment. According to Art. 15(8) these providers shall:

1) identify and verify each customer upon establishment of a business relationship and entering into a transaction while being present at the same place as the customer, if the value of the transactions of the customer exceeds 1,000 euros per calendar month or an equal amount in another currency;

2) upon mediation of a transaction between several customers, identify and verify each person participating in a transaction.

436. Article 15(6) the MLTFPA provides for special requirements that apply to currency exchange services. A provider of currency exchange services is required to identify and verify all persons participating in a transaction if the amounts exchanged in cash either in a single transaction or related transactions exceed 6,400 Euros or an equal amount in another currency.

*Identification measures and verification sources (c.5.3*)*

437. According to Art. 13(1)1) of the MLTFPA, the financial institution is required to identify a customer or a person participating in a transaction on the basis of documents and data submitted by the person and to verify the submitted information on the basis of information obtained from a reliable and independent source.

438. The documents and data to be collected for the identification of the customer are set out in Art. 23 (for natural persons) and Art. 24 of the MLTFPA (for legal persons).

Natural Persons

439. Article 23(1) of the MLTFPA stipulates that financial institutions shall identify a natural person and verify the identity of the person on the basis of a document specified in Art. 2 (2) of the Identity Documents Act or a valid travel document issued in a foreign country or a driving license complying with the conditions provided in Art. 4(1) of the Identity Documents Act[49]. A person below 7 years of age may be identified on the basis of a birth certificate specified in Art. 30 of the Vital Statistics Registration Act.

440. On the basis of Art. 2(2) of the Identity Documents Act, financial institutions shall require a natural person to produce at least one of the following personal documents: an identity card; a digital identity card; a residence permit card; an Estonian citizen's passport; a diplomatic passport; a seafarer's discharge book; an alien's passport; a temporary travel document; a travel document for a refugee; a certificate of record of service on ships; a certificate of return; a permit of return. A travel document is accepted when issued in Estonia, issued by a foreign state or an international organisation which is recognised by the Ministry of Foreign Affairs.

441. A copy shall be made of the page of an identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification of the persons financial institutions shall register the following personal data:

1) the name;

2) the personal identification code or, in the absence of a personal identification code, the date and place of birth;

[49] As determined in Article 4 (1) of the Identity Documents Act an Estonian citizen or an alien may also prove his or her identity with a valid document not specified in the Act if the name, photograph or facial image, signature or image of signature and date of birth or personal identification code of the holder are entered therein. A photograph need not be entered in a document held by an Estonian citizen or an alien under 4 years of age and a signature need not be entered in a document held by an Estonian citizen or an alien under 15 years of age.

3) the name and number of the document used upon identification and verification of persons, and its date of issue and the name of the agency which issued the document;

4) the name of the document used upon identification and verification of the right of representation, and its date of issue and the name of the issuer.

442. On the basis of information received from the customer, the financial institution shall register the address of the place of residence and the profession or area of activity of the customer.

443. The identification and verification requirements apply to (1) a person participating in a transaction performed in economic or professional activities; (2) a person participating in a professional operation; (3) a person using a professional service; or (4) a customer (Art. 23(4)). It is unclear why Art. 23(4) refers to four different categories of persons in whose respect identification and verification measures have to be applied, while Art. 13(1)1) only refers to (1) a customer and (2) a person participating in a transaction. The evaluators were informed that purpose of the MLTFPA Art. 13 is the general obligation to implement due diligence measures while the purpose of the Art. 23 of the MLTFPA is to define which documents and data has to be collected when implementing CDD measures**.**

444. Article 23(6) provides for the possibility of receiving documents certified or authenticated by a notary public or authenticated officially for verification purposes, where identification documentation cannot be received in original.

445. Articles 23(4) and (7) require that a person participating in a transaction or professional operation performed in economic or professional activities, a person using a professional service or a customer shall, at the request of an obligated person, submit documents and provide relevant information required for the application of CDD measures as well as certify the correctness of the submitted information and documents by signature. Article 23(4) and (7) of the MLTFPA facilitate the implementation of CDD requirements by notaries public, i.e.: a) the possibility to request additional information and data and b) the possibility to demand a signed certification of the information and documents which are not determined in the Notarisation and Notaries Act.

446. The identification and verification requirements are further elaborated in the FSA Guidelines. Reference is made to the checks that should be carried out when an identification document is submitted, which include, for instance, ensuring that the document is valid by referring to the expiry date; checking that the outward likeness and age of the person match the appearance of the person represented on the document; and the personal identification code matches the gender and age of the person. A copy of the page containing personal data and a photo must be made of the identity document in accordance with subsection 2 of Art. 23 of the MLTFPA.

447. The FSA Guidelines determine that the permanent or primary place of residence of the person must be registered. If it is difficult to determine a person's permanent place of residence (e.g. the person's place of residence cannot be identified or there are several), the person's habitual residence must be identified. A post office box number cannot be considered a habitual residence. In addition to the address of the place of residence of the individual, the obligated person may record other contact details, including an e-mail address, phone number, Facebook account, Skype account and other similar data, and agree on the submission of information via these telecommunications channels. FSA and service providers confirmed that this information is very important in KYC procedures.

Legal Persons

448. Article 24(1) of the MLTFPA stipulates that a financial institution shall identify a legal person and its passive legal capacity[50] and verify the information obtained. Legal persons registered in Estonia and branches of foreign companies registered in Estonia shall be identified on the basis of an extract of a registry card[51] of the relevant register. Foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by a competent authority or body not earlier than six months before submission thereof. The relevant documents for an Estonian legal person are always available from the Central Commercial Register. The Estonian authorities also clarified that an extract from the commercial register is only valid for 15 days**.**

449. The document submitted for identification shall contain at least:

1) the business name or name, seat and address of the legal person;
2) the registry code or registration number;
3) the date of issuance of the document and the name of the agency which issued the document.

*450.* According to Art. 24(3) of the MLTFPA, on the basis of the documents specified or, if the aforementioned documents do not contain the respective data, on the basis of the information received from the representative of the legal person participating in the transaction, an obligated person shall register the following data:

1) the names of the director or the members of the management board or a body substituting for it and their authorisation in representing the legal person;
2) the area of activity of the legal person;
3) telecommunications numbers;
4) the data of the beneficial owners of the legal person.

451. During the on-site visit, the evaluation team asked financial institutions to explain which information received from the representative of the legal person would be considered adequate and accurate, in those cases where official documentation did not contain the data required under Art. 24(3) of the MLTFPA. Financial institutions stated that the information would be obtained from the representative in written format and verified through different databases. The representative would also be required to certify that the information provided is accurate and valid.

[50] In the Estonian legal system the passive legal capacity of a legal person is the capacity to have civil rights and perform civil obligations. A legal person may have all civil rights and obligations, except those intrinsically human. 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. The passive legal capacity of a legal person in public law arises at the time provided in an Act.

[51] A separate registry card shall be opened for each undertaking entered in the register. The commercial register shall include the registry card, the business files, and the registry files. Among other information determined in Article 64 of the Commercial Code the following shall be entered on a registry card: the business name and registry code of the undertaking or company; the residence or registered office, and address of the undertaking or company; information on the sole proprietor; information on the suspension of the activity, seasonal or temporal activity of the enterprise of the sole proprietor; information on general partners and liquidators of the company and persons who are granted right of representation or information on members of the management board and liquidators of the company; information on procurators; the legal form of the undertaking or class of company; notation concerning entry of the shares of the company in the Estonian Central Register of Securities; date of entry; etc.

452. Article 24(5) of the MLTFPA specifies that an extract of the registry card does not have to be submitted if the obligated person has access to the data of the commercial register and the register of non-profit associations and foundations via a computer network.

453. According to Art. 24(6) of the MLTFPA, if the document or data serving as a basis for identification of legal persons cannot be received, documents certified or authenticated by a notary public or authenticated officially shall be used for verification of the identity of a person.

454. The FSA Guidelines elaborate further on the identification, registration and verification of legal persons. The identification and verification of the identity and passive legal capacity of a legal entity must be carried out, as a general rule, on the basis of the information contained in the commercial register of Estonia or another equivalent register or a copy of the registration certificate or an equivalent document (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent). Documents issued by a register or their equivalents must have been issued no earlier than 6 months prior to their submission to the obligated person (in case of foreign legal persons)..

455. Documents issued in a foreign state must be legalised or apostilled. An apostille needs to be made in accordance with the Hague Convention of 5 October 1961, *Abolishing the Requirement of Legalisation for Foreign Public Documents* (hereinafter the Convention). Documents originating from countries that have not joined the Convention need to be legalised. Documents issued by Lithuanian, Latvian, Polish, Ukrainian or Russian authorities and officials do not require legalisation or an apostille.

456. The FSA Guidelines determine that the list of reliable sources of information must be specified by the obligated person (e.g. information issued by national registers, public authorities, credit institutions, foreign missions of the Republic of Estonia and foreign missions in Estonia may be used) and do not provide for other possibilities for verification of data defined in Art. 24(3).

Legal Arrangements

457. Legal arrangements do not exist as an entity in the legal system of Estonia. With respect to foreign legal arrangements, the authorities clarified that according to the general part of the civil code, financial institutions cannot establish a legal relationship with a foreign legal arrangement. 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 obligated person. Therefore, financial institutions in Estonia may not enter into any contract or provide any service to a legal arrangement.

*Identification of legal persons or other arrangements (c.5.4)*

Criterion 5.4(a)

458. Article 13(1)2) of the MLTFPA requires financial institutions to identify and verify a representative of, *inter alia,* a legal person and verify the right of representation.

459. According to Art. 23(1) of the MLTFPA, in addition to an identity document, the representative of the legal person shall submit a document, certifying the right of representation. The financial institution shall register the same personal data as required for natural persons (See c.5.3) (the representative's name; the personal identification code or, in the absence of a personal identification code, the date and place of birth; the name and number of the document used for identification and verification of persons, and its date of issue and the name of the agency which issued the document; the name of the document used for identification and verification of the right of representation, and its date of issue and the name of the issuer).

460. Pursuant to Art. 23(5) of the MLTFPA, the representative of a foreign legal person shall, at the request of an obligated person, submit a document certifying his or her powers, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a

certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement.

Criterion 5.4(b)

461. In terms of Art. 24(1) of the MLTFPA, financial institutions are required to identify a legal person and its passive legal capacity and verify the information obtained.

462. As already stated under criterion 5.3, the financial institution is required to obtain an extract from the registry which contains:

1) the business name or name, seat and address of the legal person;
2) the registry code or registration number;
3) the date of issuance of the document and the name of the agency which issued the document.

*463.* Additionally, the financial institution is required to obtain information (either from the registry or from the representative himself) and register the following data:

1) the names of the director or the members of the management board or a body substituting for it and their authorisation in representing the legal person;
2) the area of activity of the legal person;
3) telecommunications numbers;
4) the data of the beneficial owners of the legal person.

464. The requirement to obtain information on the provisions regulating the power to bind the legal person (which would generally be found in the Memorandum and Articles of Association of a company) is covered in Art. 24(3)1) of the MLTFPA. Based on the FSA Guidelines the financial institutions are required to register the names of the executive or members of the management board and their powers and rights of representation of the legal person and the principal field of activity. If the relevant information is not indicated by the register extract or other document, the relevant information must be obtained from other relevant sources.

465. As mentioned previously, financial institutions may not provide services to a legal arrangement since these are not recognised under Estonian law.

*Identification of beneficial owners (c.5.5*, 5.5.1*, 5.5.2(a) and 5.5.2(b)*)*

466. The MLTFPA provides a definition of a beneficial owner under Art. 8, which reads as follows:

> *"(1) A beneficial owner is a natural person who, taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interest or favour or on whose account a transaction or operation is performed.*
>
> *(1¹) A beneficial owner is also a natural person who ultimately holds the shares or voting rights in a company or exercises final control over management of a company in at least one of the following ways:*
>
> *1) by holding over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;*
>
> *2) otherwise exercising control over management of a legal person.*
>
> *(2) A beneficial owner is also a natural person who, to the extent of no less than 25 percent determined beforehand, is a beneficiary of a legal person or civil law partnership or another*

*contractual legal arrangement, which administers or distributes property*[52]*, or who exercises control over the property of a legal person, civil law partnership or another contractual legal arrangement to the extent of no less than 25 percent.*

*(3) A beneficial owner is also a natural person who, to an extent not determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, and primarily in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates.*

*(4) Clause 1) of subsection (1¹) of this section does not apply to companies whose securities have been listed on a regulated stock exchange."*

Criterion 5.5

467. Article 13(1)3) of the MLTFPA requires financial institutions to "*identify the beneficial owner … on the basis of information provided in pre-contractual negotiations*[53] *or obtained from another reliable and independent source".* The evaluators note that Art. 13(1)3) does not specifically require financial institutions to verify the identity of beneficial owners. However, Art. 23(1) requires financial institutions to identify and verify the identity of a natural person, irrespective of whether the natural person is the customer or the beneficial owner. It is the view of the evaluation team that for the avoidance of any doubt Art. 13(1)3) of the MLTFPA should be amended to specify that the identity of the beneficial owner is to be verified or else refer to Art. 23(1).

468. Concerning the footnote of c.5.5, although the definition of a beneficial owner does not include the beneficiary under a policy, Art. 15(5) of the MLTFPA provides that insurance companies and brokers may verify the identity of a beneficiary under a life assurance contract after the establishment of a business relationship, but not later than upon making a disbursement or commencement of realisation of the rights of the beneficiary arising from the life assurance contract. While this provision covers the timing of verification (which is relevant under c. 5.14), it implies that the beneficiary under a policy must be identified and his identity verified.

Criterion 5.5.1

469. There is no express requirement in the MLTFPA obliging financial institutions to determine whether the customer is acting on behalf of another person. This is of particular significance where the financial institution is dealing with customer who is a natural person. Financial institutions may assume that a natural person wishing to establish a business relationship or carry out an occasional transaction is doing so in his own name and not acting on behalf of another person (especially where that other person is a natural person). They are not under any obligation to take measures with the purpose of exposing a person attempting to conceal his identity by acting through another person.

470. The absence of an express requirement in the law is in part mitigated by guidance provided under certain sections of the FSA Guidelines. Section 7.3 refers to those situations where the customer appears to be acting, wilfully or under duress, according to the instructions of another person. Section 8.2 deals with agency relationships between the customer and the underlying beneficial owner and clearly states that financial institutions must determine if the customer is acting in his own name or on behalf of another (natural or legal) person. If it is found that the

[52] Reference to legal arrangements was made in order to transpose the definition of beneficial owner in Directive 2005/60/EC.

[53] The authorities explained that within the context of the provision of certain services which involve entering into a contract, CDD information must be obtained in the course of pre-contractual negotiations regulated by Article 14 of the Law on Obligations.

customer is acting on behalf of another person, then the financial institution is required to identify the person on whose behalf the transaction is carried out. Despite the fact that Section 8.2 broadly covers the circumstances referred to under criterion 5.5.1, it may not be considered to be compliant with the criterion since the FSA Guidelines are not law or regulation.

Criterion 5.5.2 (a)

471. Article 13(1) 3) requires financial institutions to gather information on the ownership and control structure of a legal person, trust, civil law partnership or other contractual arrangement on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source. The FSA Guidelines (points 4.1.6 and 8.3.4) provide the measures to verify and understand the corporate structure (ownership and management structure of the group of companies) for the supervised obligated persons.

Criterion 5.5.2 (b)

Legal persons

472. The beneficial owner of a legal person in terms of Art. 8 is "*a natural person who ultimately holds the shares or voting rights in a company or exercises final control over management of a company in at least one of the following ways:*

*1) by holding over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;*

*2) otherwise exercising control over management of a legal person."*

473. The definition therefore includes both natural persons who ultimately own the legal persons and also those natural persons who exercise ultimate effective control over the legal person.

474. While there is no specific requirement in the MLTFPA to take reasonable measures to determine who the natural persons that ultimately own or control the legal person are (as determined in 5.5.2.b)), a combined reading of Art. 13(1) 3) and Art. $8(1^1)$ produces the same effect. According to Art. 24(3), financial institutions are required to register the data of the beneficial owner of the legal person obtained on the basis of documents specified in Art. 24(1) of the MLTFPA (extract from the registry) or, in the absence of such documents, from information received from the representative of the legal person**.**

475. During the on-site visit, the evaluation team asked financial institutions to explain which information received from the representative of the legal person would be considered adequate and accurate, in those cases where official documentation did not contain data on beneficial ownership. Reference was made to the FSA Guidelines (Advisory Guidelines Art. 8.3.1., 8.3.3.) which state that if the official documents do not indicate the beneficial owner of the entity, the relevant information must be registered on the basis of statements or a handwritten document of the representative of the entity, certifying that the information is accurate. Information would then be verified through different databases, (if the financial institution is not in a position to verify this information, the authorities indicated that the financial institution is not be permitted to establish the business relationship). According to the rules of procedures of the obligated persons the statement must be signed by the person who is representing the beneficial owner. Based on the MLTFPA and the FSA Guidelines, financial institutions may use a risk-based approach and take sufficient measures to verify the identity of the beneficial owner with the aim of being certain who the beneficial owner of a business relationship or a transaction is. It was noted that the statement is not signed by the beneficial owner himself. This raises some concern, in certain higher risk situations (e.g. when the financial institution is dealing with a complex corporate structure). In the view of the evaluators while the legal requirements are in force, further measures to improve effectiveness are still required.

Legal arrangements

476. Article 8 of the MLTFPA defines the beneficial owner of a legal arrangement as following:

> *"1) Where the beneficiaries have been determined, the natural person who is (1) a beneficiary of at least 25 percent of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, or (2) who exercises control over at least 25 % of the property of a legal person, civil law partnership or another contractual legal arrangement; and*
>
> *2) Where the beneficiaries have not yet been determined, the natural person who is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, and primarily in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates."*

477. The definition appears to broadly capture all the requirements under Criterion 5.5.2(b) and the examples provided thereunder.

478. However, as mentioned previously, legal arrangements do not exist in the legal system of Estonia. With respect to foreign legal arrangements, the authorities clarified that according to the general part of the civil code, financial institutions cannot establish a legal relationship with a foreign legal arrangement, since this is not recognised as a legal person in Estonia, i.e. to have legal capacity in its own right to be in a contractual relationship with an obligated person. Therefore, legally, financial institutions would only be in a position to establish a business relationship with or offer services to the natural persons behind the legal arrangement in their own name and for their own behalf. A contract established between a financial institution and a person representing a foreign legal arrangement would be null and void under Estonian law.

*Information on purpose and nature of business relationship (c.5.6)*

479. According to Art. 13(1) 4) of the MLTFPA, financial institutions must obtain information about a business relationship and about the purpose and nature of a transaction. While this article does not accurately reflect the requirement under c.5.6 (information about a business relationship is too generic and may be interpreted not to cover the purpose and intended nature of a relationship), Art. 3(2) of Regulation No. 10 requires financial institution to have procedures for the identification of the purpose and intended nature of business relationships and transactions prior to the conclusion of such transactions or long-term contracts. This criterion is therefore considered to be met.

*Ongoing due diligence on business relationship (c.5.7*, 5.7.1 & 5.7.2)*

480. On the basis of Art. 13(1)5) of the MLTFPA, financial institutions are required to conduct constant monitoring of a business relationship.

Scrutiny of transactions (c.5.7.1)

481. Constant monitoring includes monitoring transactions entered into during the business relationship and, if necessary, identification of the source and origin of funds used in the transaction.

482. Regulation No. 10 specifies the basis for monitoring business relationships, which must be set out in the financial institution's rules of procedure. The rules should include methods for ascertaining the area and profile of activities of a customer, procedures for monitoring and analysing transactions concluded by the customer, and other "know your customer" requirements. Simplified and enhanced measures must be distinguished. The rules must also specify limits, classes or other criteria for electronic payment instruments as well as unusual or suspicious transactions.

483. Further guidance is provided on transaction monitoring under Section 9.2 of the FSA Guidelines. Accordingly, financial institutions are required to monitor comprehensively the content and purpose of the customer's transactions and operations to identify any possible links to money laundering or terrorist financing. The obligated person must constantly assess changes in the customer's operations and whether these may raise the risk level and so that additional customer due diligence measures need to be taken. A list of typical parameters on the basis of which transactions can be selected for monitoring is given in 9.2.4.4 of the FSA Guidelines.

Up-to-date information (c.5.7.2)

484. As part of their ongoing monitoring, financial institutions are required to regularly verify data used for identification and update relevant documents, data or information.

485. Pursuant to Art. 3 and 16 of the Regulation No. 10, financial institutions' rules of procedure must specify the methods for updating data and documents which are insufficient or inaccurate or which have changed. The procedures must provide for the possibility of updating data or documents according to the risk profile of customers or material changes in the area or volume of business identified through transaction monitoring. The procedures should provide the period of time within which the updated data must be made available to all relevant units within the financial institutions.

486. The FSA Guidelines provide detailed provisions on how to update the customer's personal data and operating profile, ensuring that they are up to date and based on the customer's risk level. In particular, it makes a recommendation for financial institutions to consider meeting with all the customers and/or update the customer's personal information and activity profile at least once annually.

*Risk – enhanced due diligence for higher risk customers (c.5.8)*

487. Article 19(1) of the MLTFPA requires the application of enhanced CDD *"if the nature of a situation involves a higher risk of money laundering or terrorist financing".* Besides this general requirement, Art. 19(2) specifies three instances which are considered by their nature to present a higher risk of ML/FT: (1) where identification and verification of identity is conducted on a non face-to-face basis; (2) where there are suspicions about the truthfulness of the data and authenticity of documents submitted for identification and verification purposes or suspicions regarding the identity of the beneficial owner(s); (3) foreign politically exposed persons.

488. The enhanced CDD with respect to the instanes referred to under Art. 19(1) and (2) shall consist in one or more of the following additional measures:

1) identification and verification of a person on the basis of additional documents, data or information, which originates from a reliable and independent source or from a credit institution or a branch of a credit institution registered in the Estonian commercial register or from a credit institution, which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to this Act are in force, and if in such credit institution the person has been identified while being present at the same place as the person;

2) application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be notarised or officially authenticated or confirmation of the correctness of the data by the credit institution specified in clause 1), which issued the document;

3) making the first payment relating to a transaction through an account opened in the name of a person or customer participating in the transaction in a credit institution which has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force.

489. In all cases which present a higher risk of ML and TF, financial institutions shall apply constant monitoring of a business relationship more frequently than usually (Art. 19(4)).

490. Regulation No. 10 requires financial institutions to include in their rules of procedure a description of high risk transactions, including transactions concluded in the context of private banking and the monitoring of such transactions.

491. In order to identify higher risk scenarios, Art. 29(1) requires financial institutions to establish written rules of procedure for the assessment and management of ML/FT risks. Pursuant to Art. 14 of Regulation 10, financial institutions shall determine the risk profile of a legal person on the basis of the country where the legal person has its place of business or is registered, the type and status of the legal person, the area of activity and territory where activities are carried out, the management structures of the legal person, the beneficial owners and agents of the legal person, the type and volume of services offered by the financial institution to the legal person, sources of financing of the activities of the legal person and risk profiles of the business partners. Based on this risk profile, the financial institution is required to determine whether the application of enhanced CDD is required. There is no similar provision for natural persons in Regulation 10.

492. Section 4.6 of the FSA Guidelines provides comprehensive guidance on how to apply the risk-based approach, including a list of factors for customer, product/service and geographical risk that might be taken into consideration when assessing ML/FT risks. The additional criteria for higher than normal risk situations are, for instance, private banking or alternative payment services, where the customer is registered in a low tax region, non-resindent customers, and complex legal structurse (where it is difficult to determine who the beneficial owner/shareholder is). The Guidelines state that the customer's risk level is usually high, when after assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of ML/FT is high or considerably higher. Enhanced CDD must be appled in accordance with Art. 19, 21 or 22 of the MLTFPA.

493. In Estonia companies are not permitted to issue bearer shares. In the case of non-resident customers, the FSA Guidelines require financial institutions to determine whether the entity issues shares in bearer form and to take additional measures to mitigate the risks emanating therefrom.

*Risk – application of simplified/reduced CDD measures when appropriate (c.5.9)*

494. Article 17 of the MLTFPA permits financial institutions to apply simplified CDD measures, in the event of a low risk of ML and TF. The conditions which must be met by a customer or a product to qualify for the application of simplified CDD are set out in Art. 18 of the MLTFPA.

495. Article 17(1) of the MLTFPA determines that upon fulfilment of the conditions provided for in Art. 18 of the MLTFPA, an obligated person may conduct due diligence measures pursuant to a simplified procedure. Financial institutions must determine the appropriate scope of the simplified measures according to the nature and risk of the business relationship, the transaction or the customer. Where the obligated person decides to apply simplified customer identification it shall, at its own discretion, select the customer identification measures, as well as their scope. According to 17(3) of the MLTFPA, the obligated person must gather enough information to identify whether the transaction or customer complies with the conditions for the application of simplified due diligence. Minimum CDD (i.e. less detailed CDD) should be applied, including in circumstances where the risk of money laundering and terrorist financing is low.

496. Under Art. 18 the categories of customers and products that may be subject to simplified CDD are the following:

1. a legal person governed by public law founded in Estonia [54];
2. a governmental authority or another authority performing public functions in Estonia or a contracting state of the EEA;
3. an authority of the European Community;
4. a company of a contracting state of the European Economic Area or a third country, which is subject to requirements equal to those measures provided in MLTFPA, and whose securities are traded in a regulated securities market in one or several contracting state of the EEA;
5. a credit institution or a financial institution located in a contracting state of the EEA or in a third country, which is subject to requirements equal to those provided for in MLTFPA and are subject to supervision for compliance with such requirements.

497. Additionally, financial institutions may apply simplified CDD with respect to the beneficial owners of an official account opened by a notary public or enforcement officer of a contracting state of the European Economic Area or third country, provided that the official account is subject to due diligence measures which are in compliance with the international standards for prevention of money laundering and terrorist financing, state supervision is exercised over adherence to these requirements and the notary public or enforcement officer has and retains information about the identity of the beneficial owner.

498. Simplified CDD may also be performed with respect to life assurance contracts where the annual premium does not exceed EUR 1,000 or EUR 2,500 in the case of a single premium; a pension insurance contract which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral; a transaction is entered into in the framework of a superannuated pension scheme or another scheme allowing for such pension benefits whereby insurance premium is debited from wages and the terms and conditions of the pension scheme do not allow for assignment of the rights of a participant in the scheme.

499. An electronic money institution may also apply simplified CDD if an e-money device does not allow for reloading and the amount deposited in one e-money device does not exceed EUR 250.

500. According to Art. 18(4) of the MLTFPA, simplified CDD may also be performed with respect to a transaction when all the following criteria are met: the obliged person has concluded a written contract with a customer for an indefinite period; a payment is made through the account of a customer or a person participating in a transaction, which has been opened in a credit institution or a branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force; the obligated person has established by rules of internal procedure beforehand that the annual total value of performance of financial obligations arising from transactions of such type does not exceed the maximum limit of EUR 15,000; the obligated person registers at least the data specified in clauses 23(2) 1)-4) of MLTFPA with regard to the customer.

[54] A legal person governed by public law founded in Estonia is any legal person founded in the public interest and pursuant to a special law concerning such legal person. A legal person in public law shall not have civil rights or obligations which are contrary to its objective. A legal person in public law is similar to governmental authority, it is owned and controlled by state. The legal persons in public law are providing public services (University of Tartu, National Library, National Theatre, Guarantee Fund – (it means deposit guarantee scheme)).

501. Regulation No. 11 sets out the "*Criteria of low risk of money laundering and terrorist financing which allows the application of simplified customer due diligence measures*" and was issued on the basis of Art. 18(5) of the MLTFPA. According to the regulation, financial institutions are permitted to apply simplified CDD measures where they identify low risk transactions and establish appropriate procedures for the treatment of such transactions.

502. According to Art. 3 of the Minister of Finance Regulation No. 11, the following criteria of low risk are set out for consideration as regards persons or customers:

1. verification is possible on the basis of publicly-available information;
2. the ownership and control structure is transparent and certain;
3. the activities and accounting practices are transparent;
4. the person or customer reports to or is controlled by the authorities of executive power in Estonia or an EEA state or other authorities performing public duties or by an EC institution.

503. Article 4 of the Minister of Finance Regulation No. 11 sets out the criteria of low risk for transactions[55] and the list and examples of customers registered in more common countries or regions with low tax rates.

504. Regulation No. 10 requires financial institutions to describe low risk transactions, and procedures for the ongoing monitoring of such transactions. The FSA Guidelines further explain that where the risk is lower, financial institutions may apply simplified CDD measures but may not omit the application of due diligence measures completely. Simplified CDD may be applied (depending on the decision of the obligated person on risk factors) only on the conditions provided in Art. 18 of the MLTFPA, in accordance with the Minister of Finance Regulation No. 11. The scope of CDD measures and the data registered depend on the decision of the financial institution.

*Risk – simplification/ reduction of CDD measures relating to overseas residents (c.5.10)*

505. The categories of customers that qualify for the application of simplified CDD under Art. 18 are in most cases required to be situated in Estonia or in EEA member states, all of which are automatically considered to have laws equivalent to the MLTFPA in place through the transposition of Directive 2005/60/EC and the Implementing Directive and may therefore be

[55] *"Criteria of low risk for transactions may include the requirements that the benefits of the product or related transactions cannot be realized for the benefit of third parties, except in the case of death, disablement, reaching a predetermined advanced age, or similar events.*

*(2) In case of transactions with units of an investment fund, the criteria of low risk may include the following concurrent requirements:*

*1) customers may not exercise the benefits of transactions before the lapse of one year after the transaction was carried out;*

*2) units subject to transaction cannot be used as a collateral for another transaction;*

*3) the transaction is not carried out as an accelerated payment;*

*4) the contract provides no surrender clause.*

*(3) Transactions related to units of a mandatory pension funds may be considered to be in conformity with low risk criteria.*

*(4) In case of bank accounts belonging to natural persons, the criteria of low risk may include the following concurrent requirements:*

*1) the pension or social benefit of the natural person who is the owner of the bank account is credited to the bank account by the legal person or authority identified by the account manager;*

*2) the account is debited only up to the total amount of funds specified in subparagraph 1."*

considered to be in compliance with and to have effectively implemented the FATF Recommendations. It is to be noted, however, that the FATF does not recognise the automatic equivalence of AML/CFT requirements within the Member States of the EU. Countries are still expected to conduct some form of assessment to determine whether other EU Member States are in compliance with and have effectively implemented the FATF Recommendations.

506. The following customers/obligated persons, when situated in a third country, also qualify for simplified CDD: (1) companies whose securities are traded in a regulated securities market in one or several contracting state of the EEA (2) financial institutions (3) notaries public or enforcements officers with respect to a pooled account. As far as financial institutions and pooled accounts are concerned, they must be subject to requirements equivalent to those provided under the MLTFPA and subject to supervision for compliance with those requirements.

507. Financial institutions must exercise some form of discretion to determine whether a third country is to be considered equivalent since there is no definition of 'third country' in the MLTFPA. In order to assist financial institutions comply with this requirement, the FSA issued a circular on the publication of the Common Understanding between the EU Member States on third country equivalence[56] dated 26 June 2012. The list of equivalent countries has been published on the webpage of FSA[57] and on the webpage of FIU[58]. The circular specifies that the absence of a country from the list does not automatically indicate the existence of low-level compliance with the FATF Recommendations relegating the country to the non-equivalent category.

*Risk – simplified/ reduced CDD measures not to apply when suspicions of ML/FT or other risk scenarios exist (c.5.11)*

508. According to Art. 17(2) of the MLTFPA, simplified CDD shall not be applied if there is suspicion of ML and TF. Regulation No. 11 provides that simplified measures of the Regulation shall not be applied if it appears from publicly available information that the risk of ML and TF related to the customer or a transaction is not low

509. The MLTFPA also clearly states that enhanced CDD shall be applied if *the nature of a situation involves a high risk of money laundering or terrorist financing*. Consequently if specific higher risk scenarios apply, the simplified CDD measures may not be applied.

510. The FSA Guidelines also contain a clear statement that in a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with ML or TF at all.

*Risk Based application of CDD to be consistent with guidelines (c.5.12)*

511. In terms of Art. 14(3) of the MLTFPA, financial institutions may choose the appropriate scope of application of CDD measures depending on the nature of the business relationship or transaction or the risk level of the customer.

512. Article 29(1) of the MLTFPA requires financial institutions to establish written rules of procedure for the assessment and management of the risk of money laundering and terrorist financing (internal security measures).

[56] Common Understanding between Member States on third country equivalence under the Anti-Money Laundering Directive (Directive 2005/60/EC), available:

http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf.

[57] http://www.fi.ee/index.php?id=3375

[58] http://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/riigid-kus-kehtivad-rahapesu-ja-terrorismi-rahastamise-samavaarsed-nouded.dot

513. The MLTFPA specifies that the Minister of Finance shall issue secondary legislation for areas with low ML/FT risks in terms of Art. 18(5) of the MLTFPA and for internal rules of procedure in terms of Art. 30(6) of the MLTFPA. For such purposes, the Minister of Finance issued Regulations No. 10 and 11on 3 April 2008 which came into force on 11 April 2008.

514. The internal procedures of financial institutions shall be based on the Regulations and are required to be consistent with the guidelines of the FSA. The FSA Guidelines provide further details on the assessment and mitigation of ML/FT risks. Points 4.2.1 and 4.2.2 determine that the internal procedures of financial institutions shall be based on the MLTFPA as well as the FSA Guidelines.

515. Sectoral legislation (Securities Market Act, CrIA, Insurance Act, Payment Institutions and E-money Institutions Act, etc.) requires applicants for a licence to submit the rules of procedure specified in subsection 29 (1) of the MLTFPA to the FSA. The content and changes to the rules of procedure are controlled during on-site inspections and offsite supervision of the FSA. The FSA confirmed that the application of the risk-based approach is generally in line with their guidelines.

516. All financial institutions met on site stated that FSA Guidelines are available for them and their employees are aware of the content of the guidelines. They indicated that when preparing or updating guidelines they rely on the FSA Guidelines, information received by the FIU as well as their own experience of (procedures, best practices).

*Timing of verification of identity – general rule (c.5.13)*

517. According to Art. 14(1) of the MLTFPA, financial institutions shall apply CDD measures before the establishment of any business relationship or carrying out any transaction, unless otherwise provided by the MLTFPA.

*Timing of verification of identity – treatment of exceptional circumstances (c.5.14 & 5.14.1)*

518. The MLTFPA does not provide a general exception permitting financial institutions to verify the identity of a customer after establishing a business relationship or conducting a transaction. However, a number of specific circumstances are included, as explained below.

519. Pursuant to Art. 15(4) of the MLTFPA, a financial institution may exceptionally, at the request of a person participating in a transaction, open an account before full application of CDD measures on the condition that the account will be debited[59] after full application of CDD measures and the first payment relating to the transaction is made through the account of the same person opened in a credit institution of an EEA country or third country where rules comparable to the ones in the MLTFPA are applicable. It is unclear what constitutes an exceptional circumstance which would permit a financial institution to avail itself of this exception. Moreover, the requirement to verify the identity as soon as reasonably practicable is not included. Nevertheless, it is to be noted that the exception is subject to adequate safeguards since the account may only be debited after full CDD is completed and the first payment must originate from a bank situated in a contracting state of the EEA or in an equivalent third country. The FSA Guidelines require specific procedures to be included in the banks' internal controls to deal with these scenarios. The Estonian authorities confirmed that it is not common practice for banks to resort to such exception.

520. An insurer or insurance broker may verify the identity of a beneficiary under a life assurance contract after the establishment of the business relationship, but not later than when making a

[59] Article 713 of the Law of Obligations Act states that the debiting of an account is the making of an entry in the account which reduces the obligations of the payment service provider to the client or increases the obligations of the client to the payment service provider. The account of the client of the payment service provider shall be deemed to be debited if the payment service provider has made a debit entry in the client's account.

disbursement or commencement of realisation of the rights of the beneficiary arising from the life assurance contract (MLTFPA Art. 15(5)).

521. A credit institution may open an account pursuant to the procedure provided for in clause 67 (4) 1[60] of the Commercial Code in the name of a company being established, via a notary public authorised or on the basis of personal data automatically verified by the registrar via a computer network, provided that a share capital contribution is made to the account from an account opened in a credit institution operating in a contracting state of the European Economic Area or in a branch of a foreign credit institution opened in a contracting state, and that the account is not debited before the company is entered into the Estonian commercial register or before taking the full CDD measures. Representatives of the company should provide the credit institution with CDD information pursuant to the procedure provided for in Art. 15 (1), which includes face to face contact (and signing a settlement contract within six months after opening the account).

522. The representatives of financial institutions confirmed that rules of procedure include the procedure when verification is permitted to be completed following of the establishment of a business relationship.

*Failure to satisfactorily complete CDD before commencing the business relationship (c.5.15) and after commencing the business relationship (c.5.16)*

523. Article 15(2) of the MLTFPA states that financial institutions shall not provide services that could be used without the identification and verification of the customer.

524. According to Art. 27(1) of the MLTFPA, a financial institution is prohibited from establishing a business relationship or conducting an occasional transaction if the person participating in the transaction or the customer does not submit the documents or relevant information required for CDD purposes, or if on the basis of the documents submitted the financial institution has reasonable doubts that the situation may constitute money laundering or terrorist financing.

525. According to Art. 27(1¹), credit institutions are prohibited from signing a settlement contract if the owner of the account specified in Art. 15(4) of the Act does not submit the corresponding data and documents required for CDD purposes or if the submitted documentation gives rise to ML/FT suspicion.

526. An obligated person may refuse to conduct a transaction if a person participating in the transaction does not submit the documents or relevant information required for CDD purposes or data certifying the legal origin of the property constituting the object of the transaction.

527. Where a business relationship has already been established and the customer does not submit documents and relevant information for CDD purposes, it shall be deemed a fundamental breach of contract and the financial institution is required to cancel the contract, without observing the term of advance notification.

528. Where a contract is terminated (whether at the initiative of the customer or the financial institution) due to the inability to conduct CDD, the financial institution shall submit a report to the FIU (MLTFPA Art. 32(2) and 27(6) 3)). In such cases, the funds of the customer shall be transferred to an account opened in a credit institution registered in Estonia, in an EEA Member State or a reputable third country.

529. Article 27(6) of the MLTFPA requires obligated persons to register the following information:

[60] Formal requirements for documents submitted to the registrar and technical requirements for their submission which are necessary for computerised data processing.

1. the information on the circumstances of refusal of the obligated person to establish a business relationship or conclude a transaction;
2. the circumstances of refusal at the initiative of a person participating in a transaction or professional act, a person using a professional service or a customer to establish a business relationship or conclude a transaction if such refusal is related to the application of due diligence measure by the obligated person;
3. the circumstances of the termination of a business relationship in the event provided for in subsection (3) of this section;"

530. Criteria of 5.15 and 5. 16 are met.

*Existing customers – (c.5.17 & 5.18)*

531. There is no specific requirement to apply CDD requirements to existing customers as at the date of the entry into force of the MLTFPA.

532. The measures applicable to existing anonymous accounts and accounts in fictitious names are explained in more detail under Criterion 5.1.

***Implementation and Effectiveness***

533. The MLTFPA, as well as the Minister of Finance regulations and the guidelines issued by supervisory authorities, provide a comprehensive and structured framework for the application of CDD. The current applicable rules address various gaps identified in the 3rd Round Report. However, there are some issues which appear to still require further clarification and improvement.

534. Meetings with the financial sector indicated a relatively high-level of awareness of their customer due diligence obligations. All categories of financial institutions appeared to have developed a comprehensive understanding of preventive measures. The FSA and the FIU have provided guidelines which are available to all obligated entities. Awareness of such guidelines was found to be high. All credit and financial institutions stated that they apply a risk-based approach to CDD measures.

535. Most of the interviewed financial institutions displayed good knowledge of identification and verification requirements of the MLTFPA, the relevant thresholds, and the specific procedures applicable to some service providers or products. The evaluation team was satisfied with the descriptions provided on the identification and verification procedures which are applied to all customers and the representatives of the natural and legal persons. All prospective customers, whether natural or legal persons, are required to complete an application form which is generally available in three languages (Estonian, English and Russian). In some banks, for higher risk customers, a different application form is used, which requires prospective customers to provide more detailed information. The client application form also requires information to be provided on bearer shares where they are permitted by the statute of a foreign legal person. The evaluation team had the opportunity to view some of application forms which were made available by financial institutions. All forms contained very detailed information fields, including information on beneficial ownership, which are expected to be completed by prospective customers and signed by the customer or the representative as the case may be.

536. It was explained that the identity of resident legal customers is mainly verified on the basis of information obtained from the Commercial Register of Estonia. The issues identified under Recommendation 33 may however impact negatively on the ability of financial institutions to rely on information maintained at the Commercial Register. When dealing with non-resident legal persons documentation issued by a foreign registry is required (e.g. on the corporate structure and legal form). In those cases specified under criterion 5.3, documentation is provided in an apostilled or legalised format.

537. Most credit and financial institutions reported requiring the prospective customer or the representative to always be physically present (as required by Art. 15(1) of the MLTFPA) when establishing a business relationship or conducting a transaction. The exceptions provided for under Art. 15(4²) appear to be only resorted to on an exceptional basis.

538. The requirements on determining the beneficial owner of a legal person or structure are sufficiently understood by credit institutions. None of the credit institutions interviewed had difficulties explaining the complexities that come with the definition of beneficial ownership. It is widely understood that the ultimate natural person(s) behind the legal person must be determined.

539. Where legal persons are involved, credit institutions request the customer to provide information on every level of the corporate structure down to the natural person controlling the structure. However, it was not clearly stated what documentation they require. Credit institutions were convincing in stating that they do not enter into a business relationship with the customer unless they understand the structure of the customer and are able to identify the ultimate beneficial owners. Credit institutions appear to have advanced risk management practices in place and screening process that include the identification of beneficial owners. Some credit institutions also reported physically meeting the beneficial owners. The representatives of banks met onsite confirmed that their procedures required information to be provided on every level of the corporate structure down to the natural person controlling or owning the customer.

540. As mentioned in the analysis, it is unclear whether the legal requirements to identify the beneficial owner of a foreign legal arrangement are adequate (there are no legal arrangements in Estonia). Banks explained that they would not establish a business relationship with a foreign legal arrangement. However, they were not in a position to confirm whether this was part of the bank's policy and whether rejecting business relationships with foreign legal arrangements was a regular occurrence.

541. The representatives of the insurance sector stated that they identify the beneficial owners (of legal persons) as well as the beneficiaries of a policy. Information on the beneficiary is registered when entering into the business relationship while the verification is carried out at the time of pay-out. If payments are made, the customer is requested to provide information on the purpose of the transaction and the source of funds. The insurance companies do not consider the insurance sector to pose a high risk of ML/FT since most customers are Estonian residents, the customer is always met in person and cash payments are not accepted.

542. Knowledge and awareness of beneficial ownership requirements of financial institutions, other than credit institutions and insurance companies, varied. Most of them are aware of the requirements and have internal policies. The payment services (including money remitters) and the currency exchange sectors appeared to be the weakest in this area. In most cases, the identification and verification of beneficial owners of legal persons established in Estonia appeared to rely heavily on information provided in the client application form and checks conducted through the Commercial Register of Estonia. However, the Commercial Register of Estonia does not maintain a registry of beneficial ownership and, furthermore, as noted under Recommendation 33 it is unclear whether information maintained at the register is always up to date. In case of non-resident legal persons, most of the interviewed financial institutions explained that apostilled or legalised documentation from a foreign registry would be obtained. Additional documents may be required, e.g. shipping documents, customs documents and declarations, contracts, purchase agreements, etc. Registry-issued documents do not contain information on beneficial owners, in most of the cases, unless the shareholder himself is a natural person. Some interviewed representatives could not confirm whether their procedures required information to be provided on every level of the corporate structure down to the natural person controlling or owning the customer. Most acknowledged that the establishment of the ownership structure of the legal person can be challenging in practice in case of non-residents.

543. Financial institutions confirmed that the representative of a natural or legal person is always identified and verified and his right of representation scrutinised. However, as stated in the analysis, there is no clear obligation to determine whether a natural person is acting on behalf of another person. This was confirmed by the financial institutions interviewed.

544. Financial institutions request customers to provide information on the source of funds of the transaction as well as the purpose of the business relationship in the client's application form. Credit institutions stated that information on the source of funds is verified on the basis of reliable documents, such as contracts (purchase-sale, loan, rental, service contract), invoices, customs declarations, inheritance documents, etc. Most financial institutions request information on the source of funds as part of their ongoing monitoring procedures. The other financial institutions (including investment companies, asset management and payment services) were aware of the requirements on the source of funds and the purpose of the business relationship and have implemented adequate internal procedures. However, awareness of the requirements relating to the source of funds of transactions needs further consolidation, especially in the case of higher risk customers. It was clear from the interviews that some financial institutions only require the customer to provide information in the application form without this information being verified on the basis of documentation.

545. All interviewed financial institutions referred to ongoing monitoring procedures being in place. Such procedures are largely based on the FSA Guidelines. In general transactions are monitored using a combination of automatic processes, based on pre-defined parameters, and manual real-time screening. Examples were provided of transactions being flagged by an automatic mechanism and then checked against the business and risk profile of the customer. In some cases the customer is requested to provide further information to explain an unusual transaction.

546. All financial institutions met on site could distinguish between simplified, normal and enhanced CDD measures in the cases determined in the MLTFPA. Simplified CDD is only applied in the cases provided in the MLTFPA. Most financial institutions reported having internal procedures on the risk-based approach. As regards enhanced CDD, additional measures are used, such as the approval of the management board or enhanced monitoring. One of the financial institutions also stated that they use a special form to be filled out in case of cash transactions. In case of enhanced CDD, additional documents are required. Some financial institution use different type of client acceptance forms depending on the risk level. In most of the cases as regards Estonian customers financial institutions rely on the information of the commercial register and no additional verification is sought from independent and reliable sources. The registry is considered to be the most reliable source.

547. The evaluation team found that the level of knowledge of financial institutions on the identification of ML/FT risks and risk classification of customers is appropriate. When queried about customers or transactions considered to pose a higher risk, most of the financial institutions referred to the following categories: cash transactions, PEPs, non-resident legal persons with complex corporate structure or customers or beneficial owners situated in certain countries e.g. Russia or Ukraine, tax havens, or countries known to have a high risk of corruption. Some mentioned payment services as a risk factor in the financial market as well as risk arising from services offered through certain communication channels, such as internet and phone services.

548. Risk assessment and management within credit institutions generally falls within the responsibility of risk committees or the management board. Decisions on the general parameters for risk classification and on individual determined cases (customers) are taken by these bodies based on information and documentation made available by the compliance officer. Most financial institutions explained that the experience of senior management, best practices and information

provided by the FIU played an important role in determining the ML/FT risks faced by the institution.

549. Financial institutions providing private banking services always meet the customers in person and have detailed procedures in place to understand the purpose and nature of the business relationship. Enhanced monitoring is conducted for every customer and all transactions are checked on a daily basis.

550. All financial institutions interviewed were aware that they are not permitted to commence business relationship or perform a transaction until full CDD measures are applied and the necessary information and documents are submitted. Credit institutions reported that it can take 5-10 days to set up a business relationship depending on the nature, structure or the complexity of the customer. They also confirmed that they do not enter into a business relationship unless they understand the ownership and control structure of the customer and understand the purpose of the business relationship. The other financial institutions (including investment companies and payment services) interviewed also stated that they do not get involved in a business relationship or perform a transaction until the necessary information is received.

551. Credit institutions also confirmed that they do not enter into a business relationship with shell banks, persons listed on international sanction lists, persons whose source of funds or the type of business could harm the reputation of the institution and persons whose activities are not transparent.

552. Credit and financial institutions reported that it is their practice to terminate a business relationship if they cannot receive the necessary information from the customer or where the customer appears to be unwilling to provide the required CDD information. The financial institutions (including investment companies, asset management and payment services) interviewed stated that they would not consider filing an SAR in this case but would simply refuse to establish the business relationship.

553. The FSA informed the evaluators that they have never identified any serious deficiencies in the CDD procedures of financial institutions. Considerable efforts have been made by the FSA in order to raise awareness of payment service providers (as newcomers on the market) on the implementation of the requirements of the MLTFPA. The FSA also indicated that there is a good cooperation with the sector through the management board and the compliance officer of each institution. The Banking Association has also undertaken measures to raise awareness as regards the necessary documentation and information for CDD purposes. A sample application form was prepared for banks to ensure uniform application of CDD requirements within the banking sector.

***Recommendation 8 (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

554. In the 3rd round report, Estonia was rated "Partially Compliant" for Recommendation 8. The evaluators noted that there was no specific provision in the law requiring financial institutions to have policies in place or take such measures to prevent the misuse of technological developments.

555. In order to address the recommendation provided in 3rd round report, the Estonian authorities have introduced a specific provision in the MLTFPA to cover the requirements under Recommendation 8.

*Misuse of new technology for ML/FT (c.8.1)*

556. Pursuant to Art. 30(3) 2) of the MLTFPA, financial institutions are required to establish rules of procedure describing, *inter alia*, the risks emanating from high-risk transactions, including the risks from means of communication, computer network and other technological developments and establish the appropriate requirements and procedures for entering into and monitoring such

transactions. In addition, according to Art. 30(4)5) of the MLTFPA, the rules of procedure shall contain instructions on how to effectively and promptly determine whether or not the customer is a person conducting a transaction via means of telecommunication.

557. The employee training programmes which are envisaged under Art. 29(2) of the MLTFPA as part of the internal security framework of a financial institution should include the provision of information about modern methods of money laundering and terrorist financing and the related risks.

558. The FSA Advisory Guideline on the *Requirements regarding the arrangement of operational risk management* includes the criteria to assess the risks related to use of electronic services and new technologies. It determines that depending on the scope and volume of the company's business and the nature of the services and products offered by it, the operational risk policy shall identify the activities the purpose or contents of which have a direct or indirect impact on the organization's activities in operational risk management, including the development of new products and services, the selection of external service providers, and development activities (incl. IT). The FSA informed the evaluators that services giving rise to the risk of misuse of technological developments are also analysed in the process of granting a licence for credit and financial institutions which are subject to supervision by the FSA. If during the assessment of services or products, the FSA identifies circumstances that could present higher ML/TF risks, the FSA is empowered to apply countermeasures, such as additional reporting, limiting the volumes of some services etc. If a financial institution decides to introduce and provide services (new technologies), it must apply for approval by the FSA**.**

*Risk of non-face-to-face business relationships (c8.2)*

559. As a general rule, according to Art. 15(1) of the MLTFPA, a prospective customer is required to be present at the same place as the representative of the financial institution when establishing a business relationship or requesting a service for the first time.

560. The rule is subject to some exceptions. According to Art. 15($4^2$) the customer is not required to be present for identification and verification purpose where (1) the customer is a credit institution, insurer, investment management company, a certain type of investment fund or an investment firm which has been granted a licence in an EEA Member State or a third country which provides for preventive measures equivalent to the MLTFPA and compliance with such measures is subject to supervision; (2) a credit or financial institution establishes a correspondent relationship; (3) the customer has been identified and his identity verified by an entity referred to in (1) on the basis of documents which are equal to those required under the MLTFPA.

561. Based on the proposals made by the Estonian Insurance Association and the Estonian Banking Association, the option for the identification of persons digitally (ID card, residence permit card and digital ID card, incl. digital ID card in the Mobile ID format) was introduced within the MLTFPA. According to Art. 15($4^3$), a credit or financial institution may identify and verify the identity of a customer without being physically present on the basis of a document issued by the Republic of Estonia for digital identification in limited circumstances (i.e. when the services relate to payments which do not exceed EUR 2,000 in a calendar month). According to the explanatory memorandum of the MLTFPA if a person or customer is identified on the basis of a document meant for digital identification upon the creation of a business relationship, the identification data cannot be used by third obligated person in accordance with Art. 15($4^2$)3). The evaluators were informed that e.g. in case of outsourcing of identification duty, the service provider outsourcing cannot rely on the documents that where gathered through electronic identification.

562. In all cases, where the customer is not present for identification and verification purposes, financial institutions are required to apply enhanced CDD (MLTFPA Art. 19(2)(1)). The

additional enhanced CDD measures that are to be applied are set out under Art. 19(3) (for further details refer to criterion 5.8 of this report).

563. The Minister of Finance Regulation No 10 provides additional requirements for the application of CDD in case of non-face-to-face businesses and ongoing monitoring. The code of conduct for the application of customer due diligence measures shall specify limits, classes or other criteria for transactions carried out through electronic payment instruments or other similar instruments and unusual or suspicious transactions.

564. The FSA Guidelines also address the issue and emphasise that though it is possible in cases provided by law and instances accepted beforehand by the management board to establish a business relationship without direct contact or being present with the customer at the same place, enhanced CDD must be applied. Also, the corresponding rules of procedures must be adopted by the financial institution in order to apply such exceptions.

565. The FIU has also issued guidance (which was approved by the Governmental Committee and Advisory Committee) on CDD measures of non-face-to-face businesses. The guidance has been issued for the purpose of explaining the requirements provided for in clause 19(2)1) of the MLTFPA. It determines the required data and documentation in case of residents and non-resident and provides guidance on the conditions to be taken into account: contract for an indefinite period has been concluded with a client; no suspicions arouse by entering into customer relationship by exercising due diligence; by making transactions it is possible to ensure that it is dealt with the same person; transactions are regular and economically justified. There is a set of reliable sources for verification defined in the document.

***Effectiveness and efficiency***

566. In order to address the risk of misuse of technological developments in ML and TF schemes, several amendments have been made in the MLTFPA (Art. 15($4^2$) and ($4^3$)). On an annual basis, the FIU publishes reports on new money laundering schemes detected in Estonia. The analysis conducted by the FIU shows that the transfer of funds derived from internet fraud, such as phishing, remains the dominant trend in the area of money laundering. As money can be moved from one credit and financial institution to another very swiftly, the risk of money laundering and terrorist financing is higher in the case of business relationships created without face-to-face contact. Accordingly, the MLTFPA was amended to introduce some restrictions on the services to be offered until full implementation of face-to-face CDD. .

567. Based on Art. 30 of the MLTFPA, the rules of procedure of every financial institution are required to describe transactions presenting a higher risk level, including risks related to means of communication, computer network or other technological development and establish the appropriate requirements and procedure for entering into and monitoring such transactions.

568. The FSA has undertaken significant efforts to raise the awareness of financial institutions regarding the risks related to use of electronic services and new technologies. Several training events were organised by the FSA which also included information on the risks emanating from new technologies.

569. Credit institutions appear to have sound policies in place in order to prevent the misuse of technological developments. However, some banks explained that improvements and best practices (also mitigating risks) mainly derive from experience. Banks explained that management boards have regular meetings with compliance officers to discuss issues related to risk, including the risk emanating from new technologies. Proposals are made to the board to modify the rules of procedure where the need arises.

570. The evaluation team was informed by banks that product development procedures always cover an assessment for the ML/FT risks involved. Before introducing new products additional risk

management policies are put in place. It was also confirmed that additional customer checks are applied when offering new products. Internal training always covers the risk identified with respect to new products.

571. The FSA is of the opinion that vulnerability to the threats related to the usage of new technologies are mitigated via application of the CDD measures and segmentation of the commercial services provided by financial institutions.

572. Risks emanating from new technologies are included in the rules of procedures of those financial institutions who apply services involving new technologies (where relevant). All financial institutions were aware of the requirements with respect to non-face-to-face relationships. In general, all customers or representatives of customers are met in person and the verification of identity is carried out while the customer is physically present at the premises of the financial institution. Most of them confirmed that the rules of procedure cover the policy and procedure to identify, verify and monitor of the customer who enter into a business relationship on a non-face-to-face basis.

### 3.2.2 Recommendations and comments

**Recommendation 5**

573. The CDD requirements set out in the MLTFPA are broadly in line with the requirements under Recommendation 5. However, in order to further strengthen the CDD legal provisions, it is recommended that the authorities introduce the following express requirements within the law:

- A requirement to determine whether the customer is acting on behalf of another person (c.5.5.1).
- A clear requirement to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct CDD on such existing relationships at appropriate times (c.5.17).

574. Additionally, the authorities should provide further guidance to financial institutions to assist them in understanding direct and indirect ownership and control of a legal person/arrangement and take measures to verify such information. (c.5.5.2 (a), (b)).

575. The authorities should clarify the following requirements in the law:

- The requirement to verify the identity the beneficial owner (c.5.5).
- The requirement to identify and verify the identity of the beneficiary under the policy (c.5.5)
- The requirement 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 (c.5.7.1).

576. The authorities should also consider undertaking the following measures to improve effectiveness:

- Require financial institutions to request a beneficial ownership declaration signed by the beneficial owner in higher risk situations.
- A clear requirement to register information of source of funds and verify such information on the basis of documents in higher risk situations.
- Requiring financial institutions to include in their rules of procedure the requirement to assess the adequacy of AML/CFT systems of EEA states where the prospective customer is from or in such states.

- Requiring financial institutions to have procedures in place to identify equivalent third countries (FATF has in the past challenged the reliability of the EU list)
- Review the MLTFPA to ensure that reference to a customer, a person participating in a transaction, a person participating in a professional operation, or a person using a professional service is used consistently (especially in Art. 13(1) 1)).

577. In order to improve the effective implementation of CDD requirements, the authorities should undertake further training and awareness-raising sessions with financial institutions, especially payment service providers and currency exchange operators, in particular on issues such as the identification and verification of beneficial owners, verification of source of funds and the measures to be taken when a financial institution is unable to complete the CDD procedure.

**Recommendation 8**

578. Overall the legislation to pay special attention for financial institutions to any ML threats that may arise from new technologies is in place. Estonia also has requirements in place to address any specific risks associated with non-face-to-face business relationships or transactions.

3.2.3 Compliance with Recommendations 5 and 8

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.5** | **LC** | • No clear requirement to determine whether the customer is acting on behalf of another person (C.5.5.1);<br>• No requirement to apply CDD requirements to existing customers (c.5.17);<br>**Effectiveness**<br>• Some shortcomings in the identification and verification of beneficial owners (especially on indirect ownership and control) by certain categories of financial institutions;<br>• Some shortcoming in the identification and verification of the source of funds by certain categories of financial institutions. |
| **R.8** | **C** | |

## 3.3. Financial institution secrecy or confidentiality (R.4)

3.3.1 Description and analysis

***Recommendation 4 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

579. Recommendation 4 was rated "Largely Compliant" in the 3rd round report. The only deficiency identified was that *"the provisions allowing the sharing of information between financial institutions where this is required by R.7, R9 and SRVII are drafted in a complicated way and leave some discretion and uncertainty in interpretation which may hamper their practical application"*.

***Recommendation 4***

580. All credit institutions are bound to guarantee the confidentiality of customers' data under Section 88(1) of the CrIA [61].

> *"(1) All data and assessments which are known to a credit institution concerning the clients of the credit institution or other credit institutions are deemed to be information subject to banking secrecy."*

581. Unauthorised disclosure of such information may result in criminal sanctions (section 157 of the Penal Code) or misdemeanour sanctions (Section $134^{10}$ CrIA).

582. This confidentiality is not absolute and confidentiality obligations may be lifted in specified circumstances. Section 88(5) of the CrIA requires the disclosure of information subject to banking secrecy to the Bank of Estonia and the FSA for the performance of their duties and to courts, prosecutors and other financial supervision authorities.

583. Sections 41(1) and (2) of MLTFPA provide that Financial Intelligence Unit has the right to receive information from obliged persons regarding the circumstances, transactions or persons related to suspicion of money laundering or terrorist financing, "including any information subject to banking or business secrecy".

584. These legislative provisions are discussed in detail in Section 3.4 of the 3rd round Mutual Evaluation Report and have not changed, so therefore remain valid for the purpose of this assessment. Paragraphs 559 to 578 set out the assessors' analysis, which concludes that "there are no restrictions in the Estonian legislative framework or in practice limiting competent authorities from implementing FATF Recommendation 4 and performing their functions in combating money laundering or financing of terrorism. The FIU is able to access further information from the reporting entities. For the purpose of the fight against money laundering and terrorist financing the legislation provides specific exemptions to the access information which is subject to financial secrecy."

585. With respect to the sharing of information between financial institutions, section 34(3) MLTFPA states that the duty of confidentiality may be lifted between financial institutions solely of the purpose of preventing money laundering and terrorist financing, in certain circumstances.

> *"(3) An obligated person may give information to a third party if:*
>
> *1) the third party belongs to the same consolidation group or financial conglomerate as the obligated person specified in clauses 3 (1) 1) and 2) of this Act and the undertaking is located in a contracting state of the European Economic Area or third country where requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data;*
>
> *2) the third party acts in the same legal person or structure, which has joint owners and a joint management or internal control system, as the obligated person who pursues the profession of a notary public, attorney or auditor;*
>
> *3) the information specified in subsection (1) concerns the same person and the same transaction which is related to several obligated persons and the information is given by a credit institution, financial institution, notary public, attorney or auditor to a person operating in the same branch of the economy or profession and located in a contracting state of the European Economic Area or third country where*

[61] Article 88 of CrIA was further amended on 19 May 2014.

*requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data."*

586. These provisions allow the sharing of information between financial institutions where this is required by R.7, R.9 and SR VII, although some of the terms, namely "*same consolidation group or financial conglomerate"* and *"joint owners and a joint management"* are not defined and leave some uncertainty.

587. In the 3rd round Mutual Evaluation Report the assessors suggested that this provision should be revised; "the language should be simplified to facilitate their application in practice and further guidance should be provided."

588. This suggestion was not addressed in either of the 3rd round progress reports provided by the Government of Estonia. No information regarding actual or proposed simplification of these provisions or in relation to any specific guidance on this point has been provided by Government of Estonia in the 4th round ME Questionnaire or during the onsite visit.

***Effectiveness and efficiency***

589. During the onsite visit, Estonian authorities confirmed that, in practice, there are no restrictions limiting competent authorities from accessing information in order to perform their functions in combating money laundering or financing of terrorism.

590. In relation to sharing of information between financial institutions, regulated entities interviewed during the onsite visit confirmed that no specific guidance on this point has been provided by Government of Estonia.

591. All regulated entities who were interviewed confirmed that sharing of information between financial institutions, for purposes required by R.7, R.9 and SR VII, did occur in practice and that there was no impediment to such sharing. There was some uncertainty amongst the financial institutions regarding whether such sharing was permitted on a statutory basis or on the basis of a customer mandate. Several financial institutions stated that the ability to share such information was incorporated into standard terms and conditions of their customer relationships.

3.3.2 Recommendations and comments

592. There are no legal or practical restrictions limiting Estonian competent authorities from implementing FATF Recommendation 4 and performing their functions in combating money laundering and terrorist financing. Specific legislative exemptions allow access to information subject to banking secrecy and competent authorities are able to use these exemptions where appropriate.

593. With respect to the provisions relating to sharing of information between financial institutions where this is required by R.7, R.9 and SR VII, the Government of Estonia should simplify and clarify the language in the provisions as suggested in the 3rd round mutual evaluation report and provide further guidance to financial institutions.

3.3.3 Compliance with Recommendation 4

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.4** | **LC** | • Provisions relating to sharing of information between financial institutions where this is required by R.7, R.9 and SR.VII, are drafted in a manner that leaves some uncertainty in interpretation. |

| | | |
|---|---|---|
| | | **Effectiveness**<br>• Some uncertainty amongst financial institutions regarding whether sharing of information was permitted on a statutory basis or on the basis of a customer mandate. |

## 3.4. Record keeping (R.10)

3.4.1 Description and analysis

***Recommendation 10 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

594. Recommendation 10 was rated "Largely Compliant" in the 3rd round report. The only deficiency identified in the previous round was the absence of a requirement in law or regulation to keep documents longer than five years if requested by a competent authority.

*Record keeping & Reconstruction of Transaction Records (c.10.1*, 10.1.1 and 10.2*)*

595. Article 26 of the MLTFPA provides for the record-keeping requirements to be applied by financial institutions. The original documents, or copies thereof, obtained for identification and verification purposes are required to be retained for no less than five years after the termination of the business relationship. Information shall be registered in a manner which allows for a full and immediate reply to enquiries received from the FIU, other investigative bodies or a court.

596. Minister of Finance Regulation No. 10 requires financial institutions to implement a code of conduct for the collection and preservation of data which should be included in the rules of procedure of the institution. The code of conduct should include information and procedures regarding the following: documents and data to be used for CDD and in addition methods for and time and place of submission or updating of the data; other data recorded during CDD, the name and title of the employee who registering the data; and data on transactions and funds to be collected.

Data on transactions

597. Article 25 of the MLTFPA provides for the obligation to register the data of a transaction. Paragraph (1) of this article stipulates that at the time of the identification and verification of a customer, the financial institution shall register the date or period of time of the transaction and a description of the content of the transaction.

598. The data to be registered by a financial institution is set out under Art. 25(2). This includes:

i. in the case of an account, the type, number and currency of the account and significant characteristics of the securities or other property;

ii. in the case of a deposit of property, the deposit number and the market value of the property on the date of the deposit or a detailed description of the property where the market value of the property cannot be determined;

iii. in the case of a renting or using a safe deposit box or a safe in a bank, the number of the safe deposit box or safe;

iv. in the case of payments relating shares, bonds or other securities, the type of securities, the monetary value of the transaction, the currency and the account number;

v. in the case of a life assurance contract, the account number debited and the amount of the first premium;

vi. in the case of a disbursement under a life assurance contract, the account number that was credited and the amount disbursed;

vii. in the case of a payment mediation service, the data required under Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds;

viii. in the case of alternative payments, the names of the payer and the recipient, the payer's personal identification code, and in the absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified;

ix. in the case of any other transaction, the amount of the transaction, the currency and the account number. in case of any other transactions the type and amount of currency must be registered).

599. Pursuant to Art. 26(2), transaction data shall be maintained on any data medium (data recorded on a data medium) for a period of at least five years after carrying out the transaction. According to Art. 63 of the Criminal Procedure Code any data medium may be used as evidence during criminal proceedings.

600. It appears that the data registration and preservation requirements for transactions are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Identification data

601. According to Art. of 26(1) of the MLTFPA "*an obligated person shall preserve the original counterparts or copies of the documents specified in Articles 23 and 24, which serve as the basis for identification and verification of a person, and of the documents serving as the basis for establishment of a business relationship, for no less than five years after termination of the business relationship."* Articles 23 and 24 of the MLTFPA set out the documents and data to be registered on the basis of the CDD measures (refer to criterion 5.3 of this report for further details).

602. While Art. 26(1) specifically refers to identification data, it does not explicitly include records of account files and business correspondence. The evaluators were informed that the Accounting Act determines the obligation to preserve all business documents for 7 years which include documents which are necessary for reconstructing business transactions during audits. Article 12 of the Accounting Act is as follows:

*"(1) An accounting entity shall preserve accounting source documents for seven years as of the end of the financial year during which the source document was recorded in the accounts.*

*(2) Accounting ledgers, journals, contracts, financial statements, reports and other business documents which are necessary for reconstructing business transactions during audits shall be preserved by the accounting entity for seven years as of the end of the corresponding financial year.*

*(3) Business documents relating to long-term rights or obligations shall be preserved for seven years after the expiry of their term of validity.*

*(4) Accounting rules and procedures shall be preserved for seven years after the amendment or replacement thereof.*

*(5) An accounting entity is required to also preserve in electronic form the accounting journals and ledgers which are created electronically. The legibility of electronic information shall be ensured during the whole retention period."*

603. Based on Art. 6 of the Accounting Act a business transaction means a transaction concluded by an accounting entity, a transaction between third parties, or an event relevant to an accounting entity, as a result of which changes occur in the assets, liabilities or owners' equity of the

accounting entity. It is required to record all its business transactions in journals and ledgers within a reasonable period of time following a business transaction

604. Based on the obligation of the Accounting Act it appears that the same set of information which is determined in c. 10.2. is covered, including the account files and the business correspondence. (The business correspondence would qualify under the second category: the business documents. The infringement to preserve these documents may give rise to criminal proceedings.)

605. Article 26(4) of the MLTFPA provides for a minor exception in relation to the record-keeping requirements of identification data. Where a financial institution, for the purposes of identifying a person, obtains identification data from a database which is part of the state information system, the financial institution shall be considered to have complied with record-keeping requirements on the condition that the financial institution can demonstrate that a query was made to obtain information from the database. The financial institution shall retain records that a query has been made for a period of five years from the termination of a business relationship. If the financial institution identifies a person pursuant to Art.15($4^3$) of the MLTFPA, the information of the document used for digital identification, including the user's facial image and signature image, shall be preserved in a form which can be reproduced for a term of five years after the termination of the business relationship.

Maintenance of transaction and identification data for a longer period

606. There is no requirement in the MLTFPA for financial institutions to maintain data, information or records for a longer period if requested by a competent authority.

607. The authorities referred to Art. 215 of CCP which provides that "*The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia."*

608. The investigative bodies are listed in Art. 31 of the CCP and include the following:

> *"(1) The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Competition Board, the Military Police, the Environmental Inspectorate and the Prisons Department of the Ministry of Justice and the prison that perform the functions of an investigative body directly or through the institutions administrated by them or through their regional offices are investigative bodies within the limits of their competence."*

609. According to the authorities, by virtue of Art. 215 of the CCP, the investigative bodies, which include the FIU as part of the Police and Border Guard, may request financial institutions to keep records on identification data and transactions for a longer period of time.

610. It was noted, however, that a demand in terms of Art. 215 of the CCP may only be made within the context of criminal proceedings. The power of the FIU is therefore not absolute, and may not be extended to request a financial institution to retain data for a longer period in the course of its analytical work. Additionally, Art. 215 does not extend to supervisory authorities, which are also competent authorities for the purpose of criteria 10.1 and 10.2.

611. As a mitigating factor, the authorities referred to the obligation of financial institutions under accounting rules to maintain certain records for a period of 7 years.

*Availability of Records to competent authorities in a timely manner (c.10.3*)*

612. According to Art. 26(3) of the MLTFPA, financial institutions shall retain the documents and data pertaining to identification and verification of a customer as well as to transactions in a manner which allows for a full and immediate reply to enquiries received from the Financial

Intelligence Unit or other investigative bodies or a court. Supervisory authorities are not included in this provision.

***Effectiveness and efficiency***

613. The credit and financial institutions met on site explained that generally records are kept longer than five years after the termination of a business relationship or transaction.

614. The financial sector displayed an appropriate understanding of their record keeping obligations. Representatives of financial institutions confirmed that they maintain identification data, account files, business correspondence (transaction data, updated information, SARs and CTRs, termination of the business relationship, etc.) and other relevant documents for at least for 5 years.

615. Financial institutions also confirmed that data is available in registries which allow for a full and immediate reply to enquiries from the FIU. The FIU and the FSA also confirmed that customer and transaction records are available to them on a timely basis when a request is made. The financial institutions as well as the FIU informed the evaluators that the necessary information can be provided in 3-5 days (but the requested deadline is always included in the requests of the FIU, which are in form of precepts).

616. The supervisory authorities informed the evaluators, that as far as record-keeping obligations are concerned, no relevant implementation deficiencies were observed in the course of their inspections. None of the competent authorities mentioned delays (or problems) in obtaining all relevant data and information from financial institutions.

617. Nevertheless, there is no explicit provision to ensure that the mandatory record-keeping period may be extended in specific cases upon request of the FIU and other competent authorities (as required under c.10.1 and c.10.2*).

### 3.4.2 Recommendation and comments

618. MLTFPA and Minister Regulation no. 10 cover the record-keeping requirements for the financial institutions, but there are some minor issues in the legal texts which appear to require clarification.

619. Overall it can be stated that (and in conformity with c.10.2*), financial institutions are required to maintain *records of the identification data* submitted when conducting CDD measures (including the transaction data) and *copies of the documents confirming the customer's identity* for no less than five years after termination of the business relationship.

620. In the questionnaire, Estonian authorities state that FIU has also right to request information from reporting entity if it is deemed necessary and keep those records for longer period. During the onsite visit it was confirmed that it is the everyday practice of the obligated entities. Also in practice financial institutions keep such information longer than 5 years. According to Art. 12 of the Accounting Act each accounting entity shall preserve accounting source documents for seven years as of the end of the financial year during which the source document was recorded in the accounts. This obligation has already been force for more than 10 years.

621. The requirement to maintain identification data, account files, transaction data and business correspondence for at least five years following the termination of an account or a business relationship or longer if requested by a competent authority should be regulated by law or regulation. (In Recommendation 10.2 the requests of the competent authorities not necessarily cover criminal proceedings but also information for the analytical work of the FIU.)

3.4.3 Compliance with Recommendation 10

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.10** | **LC** | • No provision in law or regulation to ensure that the mandatory record-keeping period may be extended in specific cases upon request of competent authorities (as preventive measures). |

***Unusual and Suspicious transactions***

## 3.5. Monitoring of transactions and relationships (R. 11 and R. 21)

3.5.1 Description and analysis

***Recommendation 11 (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

622. In the third round, the evaluators found that financial institutions were not required to examine the background and purpose of complex/unusual large transactions and thus to keep a record of the written findings which would be accessible for competent authorities/auditors.

***Recommendation 11***

*Special attention to complex, unusual large transactions (c. 11.1)*

623. Article 12(1) of the MLTFPA requires an obligated person to pay special attention to the activities of a person participating in a transaction or professional operation or a person using a professional service or a customer and to circumstances that refer to money laundering or terrorist financing or the connection of which with money laundering or terrorist financing is probable, including to complex, high-value and unusual transactions which do not have any reasonable economic purpose.

624. While this article does introduce a general obligation to pay special attention to complex, unusual large transactions, it does not apply the obligation to "unusual patterns of transactions" as required by the criterion.

625. The article specifically applies to transactions which do not have any *"reasonable economic purpose"*. This may be interpreted to sufficiently apply to transactions that have *"no apparent or visible economic purpose"*, but does not clearly extend to transactions that have *"no apparent or visible lawful purpose"*. The references in the article to "circumstances that refer to money laundering or terrorist financing or the connection of which with money laundering or terrorist financing is probable" do suggest unlawful purposes, but are phrased more narrowly than the criterion.

626. Regulation No. 10 of Minister of Finance "Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance" states that credit and financial institutions must implement internal procedures that establish limits, levels and other criteria to differentiate unusual or suspicious transactions and specifically refers to a situation that is "substantially different, taking into consideration the previous behaviour of the customer, and it is not reasonably justifiable or is related to a suspicion of money laundering or terrorist financing".

*Examination of complex and unusual transactions (c. 11.2)*

627. No legislative amendments were made following the 3rd round report in relation to this criterion. The Estonian authorities referred the assessors to Art. 13(1)(4) of MLTFPA, pursuant to

which an obligated person must apply CDD measures to acquire information about a business relationship and about the purpose and nature of a transaction. They also referred to Art. 13(1)(5) of MLTFPA, which requires the monitoring of a business relationship, including monitoring transactions entered into during the business relationship, regular verification of data used for identification, updating relevant documents, data or information and, if necessary, identification of the source and origin of funds used in the transaction.

> *"(1) To perform the obligation provided in Art. 12, an obligated person shall take the following due diligence measures in economic or professional activities:*
>
> *1) ...;*
>
> *2) ...;*
>
> *3) ...;*
>
> *4) acquisition of information about a business relationship and about the purpose and nature of a transaction;*
>
> *5) constant monitoring of a business relationship, including monitoring transactions entered into during the business relationship, regular verification of data used for identification, updating relevant documents, data or information and, if necessary, identification of the source and origin of funds used in the transaction."*

628. The authorities are of the view that that the effect of these provisions is that an obligated person is required to examine the background and purpose of complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.

629. However, it appears from the drafting of the provisions, that Art. 13(1)(4) (which includes the requirement to acquire information about a business relationship and about the purpose and nature of a transaction**)** only applies at the establishment of a business relationship or prior to entering an occasional transaction (as provided by Art. 14(1) of MLTFPA).

> *"(1) An obligated person shall apply the due diligence measures provided in clauses 13 (1) 1)-4) before establishment of any business relationship or entering into any transaction, unless otherwise provided by this Act."*

630. Article 13(1)(5) requires the monitoring of transactions and *"if necessary, identification of the source and origin of funds used in the transaction".* However, identification of the source and origin of funds does not equate to examining "as far as possible the background and purpose" of such transactions.

631. Therefore, while there is a general obligation to pay special attention to complex, unusual large transactions (Art. 12(1) of the MLTFPA), the only reference to investigating the background and purpose of a transaction applies as part of CDD prior to undertaking a transaction

632. The on-going monitoring obligation in Art. 13(5) of MLTFPA, by which an obligated person might discover an unusual pattern of transactions, does not require obligated persons to then investigate the background and purpose of such transactions nor to set forth their findings in writing.

633. Article 22 of Regulation No 10 of Minister of Finance "Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance" specifies that an obligated person's internal rules of procedure must provide that an employee analyses "the circumstances that have become apparent concerning the transactions with the characteristics of transactions that are related to a suspicion of money laundering or terrorist financing". However, this obligation is not as comprehensive as "examining

as far as possible the background and purpose of such transactions" (as set out in the criterion), nor does it include a requirement to set forth findings in writing.

*Record-keeping of finding of examination (c. 11.3)*

634. No legislative amendments were made following the 3rd round report in relation to this criterion. The authorities stated that an obligated person must keep relevant findings in writing for five years and referred the assessors to Art. 27(6) (4), 26(2) and 26(3) of MLTFPA.

635. However, Art. 27(6)(4) relates specifically to information that leads to a notification to the FIU pursuant to Art. 32; and Art. 26(2) applies a 5 year limit to these records and to "documents prepared with regard a transaction". As such, neither of these provisions specifically apply to records of findings made following to the examination of complex, unusual or large transactions.

636. The authorities stated that if any "complex, unusual, large transactions and unusual patterns of transactions" are discovered then the obligated person must report such transactions to the FIU. The obligated person must then preserve the information serving as the basis of the notification, pursuant to Art. 26.

637. However, the obligation to report to the FIU and the subsequent record-keeping obligations are only applicable where there is an indication or suspicion of money laundering or terrorist financing. To be fully compliant with criterion 11.3, records of the examination of complex, unusual large transactions should be kept regardless of whether there is a suspicion of ML/TF and a notification to the FIU.

***Recommendation 21 (rated NC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

*638.* In the third round Estonia was found not have implemented any of the criteria under Recommendation 21.

*Special attention to countries not sufficiently applying FATF Recommendations (c. 21.1 & 21.1.1), Examination of transactions from countries not sufficiently applying FAT Recommendations (c 21.2)*

639. Following the findings in the 3rd round report, the Estonian Authorities introduced a new Art. 14(5) of MLTFPA, that requires an obligated person to pay higher attention to business relations or transactions if the place or residence or location of a customer or a person participating in the transaction or a person using the professional service, or the place of location of a payment service provider of a beneficiary is in a third country or on a territory where sufficient measures for prevention of money laundering and terrorist financing have not been applied, or if that country or territory does not cooperate internationally in the prevention of money laundering and terrorist financing or is a territory with a low tax rate.

640. This article appears to be broadly consistent with the requirements of the criterion, however its application is limited to a customer or person residing or currently located in one of the stipulated countries. In order to fully comply with the criterion, the article should also apply to a customer or person *from* one of the stipulated countries.

641. The obligated person must implement the abovementioned obligations into their own procedures. Minister of Finance Regulation No 10 of 3 April 2008 "Requirements for the rules of procedure established by credit and financial institutions and for their implementation and verification of compliance" requires credit and financial institutions to establish written rules of procedures which should include a code of conduct for application of CDD measures. It must contain special requirements for identification and verification of customers whose place of residence or registered office is in a country where the application of AML/CFT measures are insufficient.

642. In order to assist financial institutions comply with this obligation, the FSA issues circular letters to inform supervised entities of the content of FATF Public statements and advises the institutions to consider the risks arising from the deficiencies associated with each jurisdiction mentioned in the statements and apply according counter-measures, including application of enhanced CDD measures, to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/TF) risks.

643. These circular letters are addressed to the credit and financial institutions supervised by the FSA. The circular letters are sent by electronic post and published on the webpage of FSA. They are not distributed to financial institutions subject to FIU supervision.

644. The authorities indicated that the circular letters clearly state that reporting entities are required to pay special attention to any business relationship or transaction with the countries listed in FATF documents, especially in relation to Iran and DPRK, and to assess the ML/FT risks arising from the deficiencies associated with each mentioned jurisdiction as part of their risk-assessment procedures.

645. It is not clear in that, on discovering a transaction with no apparent economic or visible lawful purpose during monitoring of identified higher risk countries, institutions are required to examine the background and purpose of the transaction or to keep records of their findings.

646. While in practice, the discovery of such a transaction may lead to a report to the FIU and subsequent record-keeping obligations, it is not clear that records of findings that do not lead to a report to the FIU should also be kept.

*Ability to apply counter measures with regard to countries not sufficiently applying FATF Recommendations (c 21.3)*

647. The authorities stated that compliance with this criterion is achieved by way of Art. 14(5) of MLTFPA, that requires an obligated person to pay higher attention to business relations or transactions with a connection to a country or territory where sufficient AML/CFT measures have not been applied that does not cooperate internationally in the prevention of money laundering and terrorist financing. Combined with Art. 19(1) of MLTFPA (which requires enhanced due diligence to be applied in higher risk situations), this has the effect that countries highlighted in the circular letters referred to at para xx above, are subject to enhanced due diligence.

648. This is further clarified in the "Additional Measures for Preventing Money Laundering and Terrorist Financing in Credit and Financial Institutions", which states that enhanced due diligence measures must be applied in the case of persons whose country of origin has been included on the list by FATF of countries not contributing enough to the prevention of money laundering or in case of countries considered a tax-free territory or territory with a low tax rate.

***Effectiveness and efficiency***

649. All financial institutions that were interviewed during the onsite visit confirmed that in practice they do examine unusual transactions and transactions from countries which do not or insufficiently apply FATF Recommendations.

650. They also confirmed that, despite there being no specific requirements to keep records of findings, the findings of such examinations are recorded in practice, even where no report is made to the FIU.

### 3.5.2 Recommendations and comments

***Recommendation 11***

651. The Government of Estonia should revisit the provisions relating to on-going monitoring of a business relationship, to make it clear that, on discovering a complex or unusual transaction or pattern of transactions, institutions are required to investigate the background and purpose of the transaction(s) and to keep records of their findings, regardless of whether a notification is made to the FIU.

***Recommendation 21***

652. Estonia should revisit the provisions around monitoring, to make it clear that, on discovering a transaction with no apparent economic or visible lawful purpose during monitoring of higher risk countries, institutions are required to investigate the background and purpose of the transaction(s) and keep records of their findings, regardless of whether a SAR is made.

653. Estonia should revisit the provisions around monitoring, to make it clear that the obligation applies to a customer or person *from* one of the stipulated countries.

654. Estonia should ensure that the circular letters that inform financial institutions of countries not sufficiently applying FATF Recommendations are distributed to all financial institutions, including those supervised by the FIU.

### 3.5.3 Compliance with Recommendations 11 and 21

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.11** | **PC** | • The requirement to pay special attention to complex, unusual large transactions does not apply to "patterns of transactions" as required by the criterion;<br>• The requirement to pay special attention does not apply to transactions which have "no apparent or visible lawful purpose" as required by the criterion;<br>• No clear requirement to examine the nature, purpose or background when discovering a complex or unusual transaction during transaction monitoring;<br>• No clear obligation to keep records of findings that do not lead to STR. |
| **R.21** | **PC** | • Technical deficiency in relation to the application of the obligation to a customer or person *from* one of the stipulated countries;<br>• 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;<br>• No clear requirement to keep records of findings that do not lead to STR;<br>**Effectiveness**<br>• Circular letters not distributed to all financial institutions. |

## 3.6. Suspicious transaction reports and other reporting (R. 13, 25 and SR.IV)

### 3.6.1 Description and analysis

***Recommendation 13 (rated LC in the 3rd round report) & Special Recommendation IV (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

655. The reporting obligation did not cover:

- all kinds of attempted transactions;
- financing of terrorist individual and organisations;
- collecting TF funds;
- financing of Treaty offences covered by TF Convention;
- deficient reporting behaviour by savings and loan associations and insurance sector.

*Requirement to Make STRs on ML to FIU (c.13.1)*

656. The obligation to report activity suspected to be related to money laundering or terrorism financing is now laid down in Art. 32(1) MLTFPA providing that an "obligated person" (as defined in Art. 3 MLTFPA) is required to notify the FIU whenever in the performance of his economic or professional activities he has reasons to suspect that an "activity or circumstances" might be indicative of money laundering or terrorist financing or an attempt thereof. The evaluation team considers the requirement to report "activity and circumstances" indicative of ML/FT to be wide enough to cover the requirement to report suspicions that funds are the proceeds of a criminal activity. The report must be filed "immediately", or at least within two working days after the moment the event has occurred or the suspicion has risen. SARs marked "urgent" in the reporting form are treated as a priority and processed immediately

657. Before filing a SAR the reporting entities have the right to postpone a transaction or operation they consider suspicious (Art. 32(5) MLTFPA). Exception is made for instances where the transaction has an immediate character or the measure would cause considerable damage or would jeopardise the ensuing investigation. This would then give the FIU the time and opportunity to issue an order of suspension according to Art. 40 MLTFPA for an extendable period of 30 days.

658. On top of that the entities subject to the MLTFPA must notify, within the same deadline, the FIU of any cash transaction involving 32,000 EUR or an equal amount in another currency, regardless of whether the transaction is made in a single payment or several related payments. An exception is made for credit institutions to which the requirement does not apply for currency exchange transactions exceeding EUR 32,000 in cash when the institution has a business relationship with the person participating in the transaction (Art. 32(3)). A further exception is made for notaries and lawyers (Art. 32(4) MLTFPA – see Rec. 16 below).

659. The FIU issues and updates guidelines for reporting suspicious transaction relating to money laundering and terrorism financing (a copy of the guidelines may be found in Annex 2). These guidelines have no mandatory character but are intended as a recommendation to assist the reporting entities by enumerating a series of alerts that may prompt a disclosure. However, one reporting entity interviewed on-site explained that it was using these indicators unthinkingly as objective criteria automatically triggering a SAR.

660. Failure to file SARs or CTRs and to submit incorrect information is punishable as misdemeanour. Failure to report is punishable by Art. 60 MLTFPA. In case of repeat offence it is

considered a criminal offence according Art. 396 PC, punishable by a fine or imprisonment of up to 1 year.

*Requirement to Make STRs on FT to FIU (c.13.2 & IV.1)*

| | 2010 | | 2012 | | 2013 | |
|---|---|---|---|---|---|---|
| | Number of reports | Percentage (%) | Number of reports | Percentage (%) | Number of reports | Percentage (%) |
| **Financial institutions** | 10,120 | 74.1 | 8,504 | 70 | 7,856 | 70 |
| **Credit institutions** | 2,681 | 19.6 | 2216 | 18.2 | 2,055 | 18.3 |
| **Other entities** | 355 | 2.6 | 785 | 6.5 | 547 | 4.9 |
| **Professionals** | 180 | 1.3 | 165 | 1.4 | 233 | 2.1 |
| **State authorities** | 130 | 1 | 252 | 2.1 | 276 | 2.5 |
| **Foreign state authorities** | 181 | 1.3 | 221 | 1.8 | 243 | 2.2 |
| **Other** | 8 | 0.1 | 14 | 0.1 | 14 | 0.1 |
| **Total** | **13,655** | **100** | **12,157** | **100** | **11,224** | **100** |

| | |
|---|---|
| **Other** | **14** |
| **Credit institutions** | **2,216** |
| **Financial institutions** | **8,504** |
| money transfer providers | 319 |
| investment | 1 |
| insurance | 2 |
| providers and issuers of securities | 6 |
| leasing companies | 3 |
| payment service providers | 3,293 |
| currency exchange providers | 4,880 |

| | |
|---|---|
| **Other private entities** | **785** |
| Traders | 190 |
| organisers of games of chance | 582 |
| other | 13 |
| **Professionals** | **165** |
| attorneys | 9 |
| Auditors | 17 |
| enforcement officers | 2 |
| providers of other legal services | 1 |
| Notaries | 127 |
| bankruptcy trustees | 5 |
| accountants | 4 |
| **State authorities** | **252** |
| FSA, Central Bank | 16 |
| Tax and Custom Board | 41 |
| Prosecutors | 2 |
| LEAs | 190 |
| Other | 3 |
| **Foreign state authorities** | **221** |
| **Total** | **12,157** |

661. The reporting regime applies to suspicions and indications of financing of terrorism as such. This is narrower than the international standard imposing a reporting duty on funds suspected to be related or used for terrorism, terrorist acts or by terrorist organisations, beside the persons financing terrorism.

*No Reporting Threshold for STRs (c. 13.3, c. SR.IV.2)*

662. Under Art. 32(1) there is no threshold for reporting activity considered suspicious by the reporting entities (SAR). The currency transaction reporting (CTR) obligation starts from more than 32,000 EUR (Art. 32(3)).

663. The requirement to file a SAR also in case of attempted transactions is meant to be covered in Art. 32(1) where it refers to indications of attempted ML or TF as reporting ground, and in Art. 32(2) referring to the circumstances covered by Art. 27(6) 1) to 3) MLTFPA. This last provision requires a reporting entity to register and keep information

- about the circumstances of refusal by the entity to establish a business relationship or enter into a transaction,
- of the circumstances of refusal to establish a business relationship or enter into a transaction on the initiative of a person participating in a transaction or professional operation, a person using a professional service or a customer, provided that the refusal is related to the application of due diligence measures by the obligated person
- on the termination of a business relationship for failure to submit the documentation required by Art. 13(1) 1 to 4) MLTFPA. Therefore, it is clearly clarified in the MLTFPA that all attempted transactions have to be reported.

**Table 19: Breakdown of attempted transactions:**

| | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|
| account opening refused | 281 | 254 | 131 | 144 |
| customer did not want to proceed with account opening during KYC process | 26 | 26 | 9 | 17 |
| customer refused to give information during KYC process and account was not opened | 199 | 223 | 255 | 159 |
| relationship with customer was terminated | 318 | 175 | 229 | 260 |
| Refusal to carry out transaction | 115 | 94 | 37 | 10 |

*Making of ML/FT STRs regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2)*

664. The requirement to file SARs is absolute, in the sense it does not provide for any exceptions where it refers in general terms to the offence of money laundering and terrorism financing. Any tax aspect is consequently irrelevant and without impact on the reporting obligation.

*Additional Elements – Reporting of All Criminal Acts (c.13.5)*

665. Since money laundering is all-crimes offence , reporting entities are required to notify the FIU of any suspicion on criminal proceeds.

***Effectiveness and efficiency R.13 and SR. IV***

666. The following statistics were provided:

**Table 20: SARs by reporting entity**

| | 2010 | | 2011 | | 2012 | | 2013 | |
|---|---|---|---|---|---|---|---|---|
| | Number of reports | Percentage (%) | Number of reports | Percentage (%) | Number of reports | Percentage (%) | Number of reports | Percentage (%) |
| **Financial institutions** | 10120 | 74,1 | 9960 | 73,6 | 8504 | 70 | 7856 | 70 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Credit institutions** | 2681 | 19,6 | 2442 | 18 | 2216 | 18,2 | 2055 | 18,3 |
| **Other entities** | 355 | 2,6 | 571 | 4,2 | 785 | 6,5 | 547 | 4,9 |
| **Professionals** | 180 | 1,3 | 147 | 1,1 | 165 | 1,4 | 233 | 2,1 |
| **State authorities** | 130 | 1 | 194 | 1,4 | 252 | 2,1 | 276 | 2,5 |
| **Foreign state authorities** | 181 | 1,3 | 214 | 1,6 | 221 | 1,8 | 243 | 2,2 |
| **Other** | 8 | 0,1 | 8 | 0,1 | 14 | 0,1 | 14 | 0,1 |
| **Total** | **13655** | **100** | **13536** | **100** | **12157** | **100** | 11224 | 100 |

**Breakdown in 2012**

| | |
|---|---|
| **Other** | **14** |
| **Credit institutions** | **2216** |
| **Financial institutions** | **8504** |
| money transfer providers | 319 |
| investment | 1 |
| insurance | 2 |
| providers and issuers of securities | 6 |
| leasing companies | 3 |
| payment service providers | 3293 |
| currency exchange providers | 4880 |
| **Other private entities** | **785** |
| Traders | 190 |
| organisers of games of chance | 582 |
| other | 13 |

| | |
|---|---|
| **Professionals** | **165** |
| attorneys | 9 |
| Auditors | 17 |
| enforcement officers | 2 |
| providers of other legal services | 1 |
| Notaries | 127 |
| bankruptcy trustees | 5 |
| accountants | 4 |
| **State authorities** | **252** |
| FSA, Central Bank | 16 |
| Tax and Custom Board | 41 |
| Prosecutors | 2 |
| LEAs | 190 |
| Other | 3 |
| **Foreign state authorities** | **221** |
| **Total** | **12157** |

**Table 21: SARs from insurance and savings and loan associations (deficiency highlighted in the 3rd MER)**

| | Insurance companies | Savings and loan associations |
|---|---|---|
| 2008 | 2 | 1 |
| 2009 | 1 | 0 |
| 2010 | 1 | 0 |
| 2011 | 11 | 0 |
| 2012 | 2 | 0 |
| 2013 | 0 | 0 |

**Table 22: SAR triggers**

| | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|
| Indicator group: 1.1 characteristics of referring to a fictitious person in case of a natural person | 716 | 690 | 677 | 685 |
| Indicator group: 1.2 Suspicion of a legal person being a fictitious person | 317 | 226 | 196 | 235 |
| Indicator group: 1.3 Unusual documents | 104 | 48 | 37 | 77 |
| Indicator group: 2 By entering into product contracts or contracts with client | 184 | 250 | 266 | 242 |
| Indicator group: 3 By concluding transactions | 1361 | 1305 | 1086 | 953 |
| Indicator group: 4 The credit or financial institution has found out circumstances related other KYC issues | 52 | 4 | 5 | 6 |
| transaction refused | 115 | 94 | 37 | 10 |
| relationship with customer terminated | 318 | 175 | 229 | 260 |

667. The figures relating to the financial/credit sector show an acceptable and proportionate level of compliance with the reporting rules, except for the savings and loan associations. The absence of disclosures made by the insurance companies and the savings and loan associations has been partially addressed: the insurance sector has started reporting, whilst the situation has remained unchanged as far as the savings and loan associations are concerned, although sector specific training was provided by the FIU. It has to be taken into account however that the ML/TF risk in this sector is very low, as the savings and loan associations are mainly situated in rural areas and focused on financing local agricultural activities, involving relatively modest sums.

668. Under Art. 32 MLTFPA reporting duty is broad, covering both transactions or operations and facts ("activity or circumstances"), but not fully comprehensive, as it covers suspected terrorism financing only, leaving out suspicions on funds linked or related to, or to be used for, terrorism, terrorist acts or by terrorist organisations or those who finance terrorism, as required by the standards (cr.IV.1).

669. Disclosures have to be made immediately or at least within two working days. Although within the FATF criteria, it is to be regretted that the law does not provide for an up-front reporting as a rule (as the EU Directive imposes), especially in the light of the power of the FIU to immobilise the suspect assets. Also, leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness as it puts the burden on a private entity, involving its liability towards the customer, which is not covered by the safe harbour provided by Art. 35 MLTFPA. This is a responsibility that should be taken up by a public authority such as the FIU. These effectiveness concerns are somewhat attenuated by the practice of the reporting entities consulting the FIU in urgent cases.

670. As far as FT reporting is concerned, the following statistics were provided. In 2009 the FIU received in total 1,416 SARs on Terrorist Financing (26 from banks, 1,366 from Payment Service providers, 23 from Currency Exchange Offices, 1 from Notaries). In 2010 the FIU received in total 1,000 SARs on Terrorist Financing (8 from banks, 16 from money transfer businesses, 930 from payment service providers, 45 from currency exchange offices, 1 from notaries). In 2011 the FIU received in total 1,153 SARs on terrorist financing (69 from Currency Exchange Office, 10 from banks, 1,074 from payment Service Providers). In 2012 the FIU received in total 1,732 SARs on terrorist financing (409 from Currency Exchange Office, 7 from banks, 1,313 from payment

Service Providers, 1 from organiser of gambling and 2 from notaries public). The number of FT SARs is indeed remarkably high. Basically this is the result of the "automatic" reporting behaviour that is triggered by any transaction involving a jurisdiction figuring in the high risk territory list issued by the ISS. The FIU IT system allows for an expedient and easy preliminary check of the SARs, with the FIU playing an intermediary role for the ISS and without overburdening the FIU workload. The relevancy and quality of the SARs in such an automatic system is obviously low, but all in all the FIU and ISS have the situation under control. The evaluation team was informed that none of these SARs resulted in investigations, indictments or convictions since there were no sufficient grounds to initiate criminal proceedings.

***Recommendation 25 (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

*671.* The factors underlying the 2008 rating related to guidance.

*Feedback to financial institutions on STRs (c.25.2)*

672. Since 2005 the Estonian FIU has published an annual report, which contains, *inter alia*, sanitized cases, typologies and existing and emerging ML trends.

**673.** In addition the FIU is empowered by Art. 39 of the MLTFPA to issue advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing. FIU has issued guidelines to specific subsectors which the Estonian authorities have stated include guidance (general feedback) on indicators of money laundering and the financing of terrorism

674. In relation to case by case feedback, the FIU provides an annual feedback notice to each reporting entity, where an SAR has been forwarded to a law enforcement authority or a Prosecutor's Office for further investigation. The FIU also updates the reporting entity on the results of the investigation (e.g. case is closed or completed) and possible convictions/acquittals.

### 3.6.2 Recommendations and comments

***Recommendation 13 and Special Recommendation IV***

675. It is recommended to

- address the deficiency in the TF reporting obligation of art. 32(1) to comply with the broader international requirement;
- effectiveness: impose the rule of the a priori reporting duty before executing the suspect operation and shift the postponement decision to the FIU;
- continue to raise awareness of and provide training to the weakly or non-performing entities.

### 3.6.3 Compliance with Recommendations 13, 25 and Special Recommendation IV

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.13** | **LC** | • No explicit requirement to report suspicions on funds linked or related to, terrorism, terrorist acts or by terrorist organisations;<br>**Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness. |

| | | |
|---|---|---|
| **R.25** | **C** | |
| **SR.IV** | **LC** | • No explicit requirement to report suspicions on funds linked or related to terrorism, terrorist acts or by terrorist organisations;<br>**Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness. |

***Regulation, supervision, guidance, monitoring and sanctions***

## 3.7. The supervisory and oversight system - competent authorities and SROs / Role, functions, duties and powers (including sanctions) (R. 23, 29, 17 and 25)

3.7.1 Description and analysis

*Authorities/SROs roles and duties & Structure and resources*

***Recommendation 23 (23.1, 23.2) (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

In the 3rd round report Recommendation 23 was rated LC based on the following underlying factors:

- There were no legal provisions to prevent persons with a prior conviction for terrorist financing from holding or being the beneficial owner of a significant or controlling interest or holding a management functions;
- For financial institutions which were not supervised by the FSA there were no registration requirements.

*Regulation and Supervision of Financial Institutions (c. 23.1); Designation of Competent Authority (c. 23.2)*

676. Article 47 provides for the AML/CFT regulation and supervision of financial institutions.

677. The FSA is responsible for the AML/CFT supervision of credit and financial institutions which are subject to the supervision of the FSA under the FSA Act and legislation adopted thereunder (Art. 47(2)). The FSA is the single financial regulator in Estonia responsible for the supervision of:

- Credit institutions
- Payment institutions
- E-money institutions
- Investment services providers
- Fund management companies
- Depositories
- Pension funds management companies
- Life Assurance Companies

678. The FSA exercises AML/CFT supervision pursuant to the procedure provided for in the FSA Act.

679. The FIU is responsible for the AML/CFT supervision of other financial institutions (Art. 47(1)), which comprise the following:

- Loan and Savings Associations
- Consumer credit providers
- Pawn brokers
- Leasing Companies
- Providers of services of alternative means of payment
- Bureaux de change

680. The FIU exercises its supervisory functions pursuant to the powers set out in the MLTFPA as explained later on in this section of the report.

681. In terms of Art. 47(5), the FSA shall cooperate with the FIU for the purpose of ensuring compliance with the provisions of the MLTFPA. The FSA is also required to submit information to the FIU annually on the number of off-site and on-site inspections carried out in the preceding year, the breaches detected and the sanctions imposed for such breaches (Art. 49(2)).

*Recommendation 30*

*Adequacy of Resources (c. 30.1); Professional Standards and Integrity (c. 30.2); Adequate Training (c. 30.3)*

FSA

682. The FSA is established as an autonomous agency pursuant to Art. 4 of the FSA Act. It has its own independent budget, with funding received from supervised entities through a scheme of supervisory charges based on capital and volume of business. At the time of the onsite, the FSA employed 73 staff, comprising of financial auditors, financial analysts, IT-specialists, lawyers, an actuaries and experts in financial services.

683. The Prudential Supervision Division of the FSA is responsible for market entry, licensing and operational risk. The Business Conduct Supervision Division is responsible for AML/CFT supervision, management information systems and integrity issues. Within the Business Conduct Supervision Division, an AML Unit has been created. Given the number of entities licensed by the FSA, the AML Unit appears to be adequately staffed and resourced, with 3 members of staff responsible for AML supervision, supported where necessary by other departments.

684. Article 30 of the FSA Act sets out the requirements for employees of the Supervision Authority, including necessary education, sufficient experience and professional qualifications to perform their duties and an impeccable professional and business reputation. Persons under investigation for or accused of a criminal offence or persons with a criminal record are prevented from being employed by the FSA, along with persons involved in bankruptcy, compulsory dissolution or revocation of activity licences. All staff are subject to a probationary period of up to six months.

685. Article 34 of the FSA Act requires that FSA employees must maintain confidential for an indefinite time any information received in the course of performing their duties.

686. FSA staff involved in AML/CFT regularly participate in relevant courses organised by the UK and US authorities, as well as regional training courses and seminars. For example:

- May 2009 – AML/CFT Workshop for Supervisors in Vienna (1 person);
- January 2010 – AML/CFT in financial services in Cyprus (1 person);

- January 2010 – Anti-Corruption measures in Turkey (1 person);
- May 2010 – AML Risk-Based supervision in NY (1 person);
- November 2010 – ML/TF Typologies (Cybercrime) in Moscow (1 person);
- February 2011 – Conference on prevention of corruption and AML in Tallinn (1 person);
- October 2011 – ML/TF Typologies in Tel Aviv (1 person);
- May 2012 – AML Conference (FATF standards) in Riga (1 person);
- March 2012 – Conference on prevention of corruption and AML in Tallinn (1 person);
- September 2012 – Risk-Based supervision course in London (1 person);
- September 2012 – Review of FATF standards in Strasbourg (1 person);
- November 2012 – Electronic Money and Anti-Money Laundering in London (1 person);
- January 2013 - Workshop on money laundering and the financing of terrorism in Macedonia (1 person);
- February 2013 – AML risk and trends course in Estonia (3 persons);
- April 2013 – AML and Market regulation course in SEC in USA (1 person);
- November 2013 – AML training seminar on PEP in Serbia (2 persons);
- February 2014 – Conference on prevention of corruption and AML in Tallinn (1 person).

FIU

687. The FIU is an independent structural unit of the Police and Border Guard Board, pursuant to Art. 36(1) of the MLTFPA. The FIU is funded as any other unit within Central Criminal Police and Art. 36(3) of the MLTFPA requires the Police and Border Guard Board to provide the FIU with sufficient funds for performance of the functions provided by law.

688. The FIU has its own permanent staff (currently 18), a dedicated database and access to all available information which is necessary to perform their duties. At the time of the onsite, the FIU had 4 staff in its Supervision Division responsible for supervising obliged persons' compliance with the MLTFPA (both financial institutions and DNFBPs). These staff also have non-supervisory responsibilities, so that staffing at the FIU does not appear to be adequate when considering its supervisory responsibility.

689. It is worth noting that, pursuant to Art. 45(4) of the MLTFPA, the supervisory powers available to the FIU may also be exercised, jointly with the FIU, by a member of the Security Police Board who is nominated to act as a contact person between the Security Police Board and the FIU. This has not occurred in practice.

690. Article 44 of MLTFPA requires that only a person with impeccable reputation, the required experience, abilities and education, and high moral qualities may be appointed as an official of the Financial Intelligence Unit. Officials of the Financial Intelligence Unit are required to maintain the confidentiality of information made known to them in the course of their official duties, including information subject to banking secrecy, even after the performance of their official duties or the termination of a service relationship connected with the processing or use of the information.

691. The staff of the FIU is regularly provided with relevant training for combating ML and TF at both domestic and international level. During 2009-2012 FIU staff participated in the following AML/CFT specific training seminars:

**2009**

- 2 FIU officials participated in the training seminar "Financial companies economic activities" (organised by the University of Tartu)
- 2 FIU officials participated in the training seminar "Administrative procedure I" and "Administrative procedure II" (organised by the Preismann Trainings)

**2010**

- 3 FIU officials participated in the training seminar "Administrative procedures and state supervision"

**2011**

- 1 FIU official participated in the training seminar "Misdemeanour procedures"
- 2 FIU officials participated in the training seminar "code of administrative court procedure"

**2012**

- 1 FIU official participated in the training seminar "Auditing projects financed by structural funds"

*Authorities' powers and sanctions*

***Recommendation 29 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

692. In the 3rd round report, the evaluators noted that there was no explicit provision empowering the FIU to compel the off-site production of records from supervised entities for supervisory purposes absent a suspicion of ML/FT.

*Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1); Authority to Conduct AML/CFT Inspections by Supervisors (c. 29.2); Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1); Powers of Enforcement & Sanction (c. 29.4)*

693. Article 48 of the MLTFPA sets out the powers of supervisory authorities, which include the right to carry out on-site inspections and obtain documents, information and oral or written explanations:

> *"(1) The supervisory authority has the right to inspect the seat or the place of business of obligated persons. The supervisory authority has the right to enter a building and room that is in the possession of an obligated person in the presence of a representative of the inspected person.*
>
> *(2) In the course of an on-site inspection the supervisory authority has the right to:*
>
> *1) without limitations inspect the required documents and data media, make extracts, transcripts and copies thereof, receive explanations regarding them from the obligated person, and monitor the work processes;*
>
> *2) receive oral and written explanations from the obligated person being inspected, members of its directing body or employees.*
>
> *(3) The supervisory authority has the right to, without carrying out any on-site inspection, demand by a precept that the obligated person submit information required for inspection."*

694. This article allows the FSA and the FIU to inspect "the seat or the place of business of obligated persons" by entering "a building and room that is in the possession of an obligated person". There

are no limitations relating to timing or prior notice, nor any limitation relating to the purpose of the inspection.

695. The article allows the FSA and the FIU to "without limitation" inspect documents and data and make copies thereof. It also allows the FSA and the FIU to ask for explanations of both documents and data inspected and also more generally.

696. In relation to off-site supervision, the article allows the FSA and the FIU to demand that the obligated person submit information required for inspection. There is no legislative provision or guidance defining "information required for inspection" in Art. 48(3). However, the FSA confirmed that this might include any information concerning the obligated person's compliance with the MLTFPA. In practice, questionnaires used by the FSA to conduct off site supervision require obligated persons to provide both descriptions and copies of internal policies procedures and controls.

697. These provisions appear to contain all elements required by the criterion.

698. By virtue of Art. 47, the supervisory powers in the MLTFPA are exercisable by the FSA and the FIU in relation to the regulated entities for which they are responsible. However, the authorities confirmed that the supervisory powers set out in MLTFPA are not exercised by the FSA. Rather, the FSA exercises supervisory powers set out in various sectoral legislation and in the FSA Act. This is enabled by Art. 6 of the FSA Act, which provides that the functions of the Supervision Authority in fulfilling the objectives of financial supervision are to perform the functions arising from the (inter alia) the MLTFPA.

699. These sectoral provisions also contain powers enabling the FSA to undertake supervision, including access to records, documents or information and the conduct of onsite inspections.

700. These powers are set out in:

- the CrIA, Articles 99 and 101;
- the Insurance Activities Act, Articles 170 and 175;
- the Investment Funds Act, Articles 286 and 292;
- the Securities Market Act, Articles $230^3$ and 232;
- the Payment Institutions and E-money Institutions Act, Articles 95 and 97.

701. For instance, the CrIA allows for the FSA to conduct an onsite inspection when, *inter alia* "there is need to perform other supervisory duties".

702. An inspection may be carried out at the credit institution, a company belonging to the consolidation group of a credit institution or a subsidiary of a foreign credit institution.

703. An inspection must, unless there is good reason, be preceded by an order to the institution, at least 3 days prior to the inspection, which sets out the purpose, extent, duration of the period and time of the inspection.

704. During on-site inspection, the FSA may enter all premises; request suitable working conditions; study documents and media and make copies thereof; and monitor the work processes without restrictions. The FSA may also demand oral and written explanations from the managers and members of staff of the person being inspected.

705. In relation to off-site supervision, the CrIA allows for the FSA to demand information, documents and oral or written explanations concerning facts relevant to the exercise of supervision. Such demands can be made of a wide range of persons, including staff and

management of the institution; staff and management of other institutions in the same consolidation group; foreign subsidiaries; and, where justified, "third persons".

706. The other sectoral provisions contain nearly identical powers. However, in relation to off-site supervision, the Investment Funds Act provides the power to demand explanations from third parties (Art. 286(1)(10) without the "where justified" limitation that is included in the other legislation. Similarly, in the Securities Market Act, the power to obtain information, documents and explanations applies to "any natural or legal person" without limitation.

707. These sectoral provisions contain broadly equivalent powers to Art. 48 MLTFPA, although generally they provide more detail and have wider application. Inspections pursuant to the MLTFPA are limited to premises in the possession of the obliged person, whereas the sectoral legislation extends to other companies in the same consolidation group. Similarly, demands for explanations pursuant to the MLTFPA are limited to the obliged person, whereas the sectoral legislation extends to a number of other parties, including other members of the consolidation group and "third persons".

708. On the other hand, Art. 48 MLTFPA contains no requirement to provide prior notice of an inspection, a requirement that appears in the sectoral legislation.

709. The effect of the various provisions is that the FSA has sufficient powers to demand free of charge information, documents and oral or written explanations concerning facts relevant to the exercise of supervision, including supervision of compliance with the MLTFPA, and to conduct onsite inspections.

710. The power to "study documents and media necessary for exercising supervision, make excerpts and copies thereof and monitor the work processes without restriction" during an onsite inspection appears sufficiently broad to enable on-site sample testing.

711. In relation to Criterion 29.4, both the FSA and the FIU have powers of enforcement and sanction against financial institutions, pursuant to the MLTFPA and the various sectoral laws. The FIU's sanctioning powers are somewhat limited. Powers of sanction are described under Recommendation 17, including a lack of sanctioning power with respect to individuals.

***Effectiveness and efficiency (R. 23 [c. 23.1, c. 23.2]; R. 29, and R. 30 (all supervisors))***

712. All financial institutions are supervised, either by the FSA or the FIU, and there are sufficient statutory powers to enable the effective supervision of compliance with AML/CFT requirements.

FSA

713. Staffing at the FSA appears to be adequate and the exercise of statutory powers in relation to on-site and off-site supervision appears to be reasonably comprehensive and effective.

714. Sectoral laws require that the FSA carry out on-site inspections parent companies of consolidated groups at least once every two years. Alongside this, a comprehensive risk based model is used to determine its AML/CFT supervisory priorities and to plan relevant actions, including an annual AML/CFT on-site inspection programme.

715. The risk model is based on a number of risk factors, including the size of the institution, the type of business conducted and its SAR reporting behaviour. FSA staff undertake a threat analysis and vulnerability assessment for each institution which considers a number of factors including the findings of analytical work conducted by other departments and off-site monitoring; findings identified during previous on-site inspections; information from the FIU; and assessments of the financial institutions' AML/CFT preventive measures and risk appetite.

716. The result of this process is an annual AML/CFT on-site inspection programme, which is agreed by the FSA management board and implemented alongside regular off-site monitoring and reactive action as and when necessary.

717. On site supervision is conducted on notice, with the obliged entity receiving between 1 day and 2 weeks' notice (depending on the size and risk profile of the institution).

718. FSA supervisory staff require information to be delivered in advance of the inspection, meaning that some processes and procedures may be reviewed prior to the inspection itself. The onsite inspection is usually conducted by 2 staff members who visit the premises of an obliged entity for up to 2 weeks.

719. Staff use an internal methodology and templates when planning and undertaking an onsite inspection. These contain objectives and activities to be undertaken (e.g. sample testing, mandatory questions, interviews, etc.). FSA staff interviewed confirmed that all aspects of AML compliance obligations are reviewed during an onsite inspection, including sample testing of files and documents.

720. Supervisory staff ask for information about the client base and/or the client list in advance of the inspection. Sample testing of files while on site comprises those business relationships identified by supervisory staff as presenting a higher ML/TF risk or otherwise selected on the basis of turnover, volume and length of relationship.

721. The sectoral laws provide that the FSA must prepare a report that summarises the findings of the on-site inspection. A draft version is sent to the obligated person and the final version takes into account the comments made to the draft. This is submitted to senior management and then to the Management Board, who make the decision on whether to apply a sanction.

722. Where remedial action is required (e.g. by way of a precept), a review of the sufficiency of the action subsequently taken is incorporated into the ongoing supervision of the obliged person.

723. Offsite supervision is undertaken by way of questionnaires issued to obligated persons, which require them to provide information about their internal policies, procedures and controls as well as copies of relevant material. Questionnaires are issued pursuant to the various sectoral legislation (eg. CrIA Art. 99(1): "…*the Financial Supervision Authority has the right to demand free of charge information, documents and oral or written explanations concerning facts relevant to the exercise of supervision*…")

724. Questionnaires may be general in nature, covering a range of obligations, or targeted specifically at areas of higher risk that may be identified through the onsite inspection programme or from external intelligence sources. By way of example, a recent set of questionnaires has focussed on controls in relation to transaction monitoring and high risk jurisdictions.

725. Responses to questionnaires are reviewed by supervisory staff and findings reported to senior management for proposed sanction where necessary and/or incorporated into the risk model described above.

726. The effectiveness of the supervisory programme is reviewed by an independent internal audit department, who ensure that (inter alia) the examination process is being carried out according to agreed plan and the conclusions and statements in the examination reports are based on legitimately collected evidence. Findings (if any) are reported to the FSA management board.

FIU

727. The FIU has 18 permanent staff, with 4 staff involved in supervision for compliance with MLTFPA. These supervisory staff are not specialists in specific sectors, but rather have responsibility across all sectors. They also have non-supervisory responsibilities, which impacts upon the adequacy of available supervisory resources.

728. During interview, FIU staff suggested that supervision was focussed on ensuring adequate SAR reporting in order to add value to the analytical function of the FIU.

729. The FIU uses a different risk model to the FSA in order to determine its supervisory priorities and to plan on-site and off-site actions. Onsite supervision is generally undertaken for 2 purposes: awareness raising visits to members of a subsector (generally repeated every 3 to 5 years) and targeted on-sites to individual entities selected due to intelligence collected, complaints or SAR reporting behaviour. Supervisory resources are thus mainly focussed on individual entities that are highlighted by receipt of adverse information, with less consideration of the inherent ML/TF risks of subsectors.

730. Onsite inspections are carried out by at least 2 staff members. On-site inspections are usually conducted on notice, although not when there is a risk that advance notice may inhibit the effectiveness of the on-site inspection.

731. The obliged entity is normally required to deliver information in advance of the inspection. This means that some analysis is conducted by FIU staff prior to the inspection itself.

732. There is no internal methodology or "check-list" used by staff in planning or undertaking an onsite inspection. FIU staff stated that the contents of an onsite inspection are always consistent and include all aspects of AML compliance obligations, including sample testing.

733. Following an onsite inspection, an inspection report is prepared by staff, summarising the finding of the inspection. This is given to the obliged entity for comment. Consideration of misdemeanour action is the responsibility of the individual staff member, but the Head of the FIU makes the decision on whether to issue a precept. There are no specific decision making criteria in this regard. FIU staff stated that, in the case of "awareness raising" inspections during 2008-2010, the policy was to be more lenient in relation to compliance failures. This was because the inspection is often the entity's first contact with the FIU and the entity was often unaware of its obligations.

734. With regard to off-site supervision, historically the FIU used questionnaires and surveys primarily to identify which entities were undertaking activities that are subject to AMLCFT obligations. Use of this tool reduced from 2010, once these entities were identified.

735. Staffing at the FIU does not appear to be adequate to effectively carry out its supervisory responsibilities when considering its supervisory responsibility for both financial institutions and DNFBPs.

***Recommendation 17 (rated PC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

*736.* In the 3rd round report, Recommendation 17 was rated Partially Compliant based on the following factors:

- The general provisions of the CrIA did not provide a clear basis to issue precepts regarding violations of AML/CFT obligations which were not directly sanctionable under Art. 57ff of the MLTFPA.
- The sanctioning regime placed sanctions at one remove, in that a precept first needed to be issued before formal sanctions.
- The FIU had no power to withdraw or suspend registration of FIs for AML/CFT reasons.

*Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Range of Sanctions—Scope and Proportionality (c. 17.4) Designation of Authority to Impose Sanctions (c. 17.2)*

737. There is a broad range of sanctions that can be applied in relation to breaches of AML/CFT requirements.

738. Chapter 7 of the MLTFPA establishes sanctions against obliged persons for failure to comply with AML/CFT requirements. These provisions were extended following the 3rd round MER, in order to provide direct sanctioning in response to a wider range of violations.

739. Articles 57 to 63 set out direct sanctions for violation of specified requirements and contain sanctions ranging from 800 to 1,200 euro[62] or detention and for individuals and 20,000 to 32,000 euros for legal persons. These include:

- failure to comply with identification requirements;
- violation of requirements for collecting information;
- violation of requirements for the application of enhanced due diligence measures;
- violation of requirements for application of enhanced due diligence measures; opening an anonymous account or savings book;
- violation of requirements to register and preserve data;
- failure to submit and late submission of mandatory information;
- violation of requirements to constantly monitor business relationships;
- failure to report suspicion of money laundering or terrorist financing and submission of incorrect information;
- unlawful notification of information submitted to FIU;
- failure to apply internal security measures;
- violation of requirements for correspondent banking; and
- violation of obligations of providers of payment services.

740. While sanctions are available for a wide range of failings, the range of fines does not appear to be particularly effective, proportionate or dissuasive (e.g. the maximum fine that may be imposed on a bank is 32,000 EUR).

741. Article 65 states that extrajudicial proceedings for any of these misdemeanours may be conducted by the FIU on behalf of the PBGB or the FSA.

742. Article 54(5) of the FSA Act states that FSA may publicise any misdemeanour rulings where this is necessary for the protection of investors, clients of financial supervision subjects or the public or for ensuring the lawful or regular functioning of the financial market. It is not clear whether the FIU has similar powers.

743. In addition to this direct sanctioning, the FSA may apply indirect sanctions by way of issuing precepts pursuant to the various sectoral acts. For instance, Art. 103 of the CrIA provides that the FSA has the right to issue a precept if:

> "*1) violations of the requirements of this Act and laws specified in sub Art. (2) and clause 6 (1) 7 of the Financial Supervision Authority Act and legislation adopted on the basis thereof are discovered upon exercising supervision.*"

744. Article 6(1)((7)) of the FSA Act reads:

> "*7) perform the functions arising from the Guarantee Fund Act, the Money Laundering and Terrorist Financing Prevention Act, the International Sanctions Act and legislation issued on the basis thereof;*"

[62] According to the PC Art. 47 a fine unit is equal to four euros.

745. Such a precept in relation to a credit institution may:

- prohibit certain transactions or activities from being conducted or to establish restrictions on their volume;
- demand amendments of the internal rules;
- demand removal of the manager (in the case where the person is not *fit and proper* and cannot hold managerial positions in the financial field);
- demand suspension of an employee from work (in the case where the person is not *fit and proper* and cannot hold current positions in the financial field);
- demand compliance with legislation regulating the operation of the credit of financial institution.

746. Article 104 of the CrIA states that in the event of a failure to comply with or inappropriate compliance with a precept, a penalty may be imposed, in the case of a natural person, up to 1,200 euros for the first occasion and altogether up to 4,800 euros for each subsequent occasion and, in the case of a legal person, up to 3,200 euros for the first occasion and altogether up to 48,000 euros for each subsequent occasion [63].

747. The other sectoral legislation contains similar provisions with equivalent effect.

748. In relation to financial institutions supervised by the FIU, the FIU has the right to issue precepts and other administrative acts in order to perform the functions arising from the law, in accordance with the provisions of Art. 38 of MLTFPA. The FIU may issue any precept to ensure that an obligated person comply with all the requirements under the MLTFPA. Failure to comply with a precept may result in a penalty payment of up to 1,300 euros for a first occasion and up to 6,000 euros for each subsequent occasion.

749. In relation to revocation of licenses, Art. 17(12) of the CrIA sates that the FSA may revoke an authorisation if a credit institution violates the procedures established by legislation for the prevention of money laundering or terrorist financing. Similar provisions exist for other institutions in sectoral legislation.

750. For FIU-supervised entities, removal from the register is available following conviction for specified crimes (see Art. 55) and upon repeated or considerable violations of MLTFPA obligations. Article 55(2) also allows for registration to be suspended for 6 months at the request of the FIU.

*Ability to Sanction Directors and Senior Management of Financial Institutions (c. 17.3)*

751. In relation to this criterion, the authorities referred to Art. 14(1) of the Penal Code, which states the following:

> *"1) In the cases provided by law, a legal person shall be held responsible for an act which is committed in the interests of the legal person by its body, a member thereof, or by its senior official or competent representative."*

752. Article 14(1) clearly refers to corporate liability, where the legal person is held responsible for the actions of directors, senior officials or representatives carried out in the interest of the legal person. However, the requirement under Criterion 17.3 refers to the extension of sanctions to the directors and senior management when a financial institution is found to be in breach of AML/CFT obligations.

753. In conclusion, the evaluation team is of the view of that this criterion is not met.

[63] Article 104 of CrIA, was amended on 19 May 2014.

*Effectiveness of Sanctions*

754. Decisions on FSA sanctions are made by the FSA Management Board, on receipt of supervisory findings from staff. The institution subject to the proposed sanction is given an opportunity to make submissions prior to the decision and legal advice is usually obtained by the management board.

755. In relation to sanctions, the FSA has commenced disciplinary actions as follows:

- 2009: 2 warning letters and 2 precepts

  (issued to a credit institution and a branch of an overseas credit institution)

- 2010: 2 warning letters and 2 precepts

  (issued to an investment firm and a life insurance firm)

- 2011: 2 warning letters and 2 precepts

  (issued to a credit institution and a branch of an overseas credit institution)

  1 withdrawal of licence

  (with respect to a payment service provider).

- 2012: 3 warning letters and 3 precepts

  (issued to 2 investment firms and a payment service provider)

- 2013: 1 warning letter, 1 oral warning, 1 precept and 1 removal of compliance officer

  (issued to 1 credit institution and 1 payment service provider).

756. The assessors were informed that the sanctions related to breaches of internal procedures and some minor shortcomings in applying CDD measures.

757. Although a wide range of potential sanctions are available to the FSA, including direct sanctioning for AML breaches (which is a newly introduced sanction since the 3rd round MER), a more limited range of sanctions appears to be used in practice, consisting mainly of precepts (enforceable remedial action). No action has been taken against senior managers in the period covered by this report, nor have any public sanctions or fines been applied to financial institutions, decreasing the dissuasive effect of sanctions imposed.

758. During the onsite visit, Estonian authorities suggested that the lack of financial penalties was the result of a robust AML/CFT culture in regulated entities meaning that there were no circumstances arising where a financial penalty was a proportionate response. However, as indicated under Recommendation 5, there were some shortcomings in the identification and verification of beneficial owners (especially on indirect ownership and control) and source of funds by certain categories of financial institutions met on-site.

759. Similarly, Estonian authorities suggested that disciplinary action taken are not made public as matter of course, but rather only where such publication is considered to be in the public interest. They further suggested that no such circumstances have arisen.

760. It is not clear whether the FIU can make public its disciplinary actions.

761. Decisions on FIU sanctions are made by the Head of the FIU, on receipt of supervisory findings from staff.

762. The FIU commenced the following misdemeanour proceedings against financial institutions:

2009: 20 against financial institutions

1 against a credit institution

2010: 10 against financial institutions

2011: 1 against a financial institution

2 against credit institutions

2012: 1 against a financial institution

1 against a credit institution

2013: 11(no breakdown available)

763. The FIU did not provide a further breakdown of the type of financial institutions that were subject to misdemeanour proceedings. The FIU did not provide information as to the nature of the misdemeanours and the reason why the FIU conducted proceedings against credit institutions (rather than the FSA).

764. The Estonian authorities stated that that misdemeanour proceeding carried out by FIU usually entail a fine and that the average individual fines and total fines imposed were as follows, although it should be noted that these figures include both financial institutions and DNFBPs under FIU supervision:

2013 – 190 EUR per fine (2,100 EUR in total)

2012 – 580 EUR per fine (5,220 EUR in total)

2011 – 123 EUR per fine (1,228 EUR in total)

2010 – 1087 EUR per fine (14,135 EUR in total)

2009 – 579 EUR per fine (31,300 EUR in total)

765. It is the view of the evaluation team that the average individual fines imposed is too low, especially those imposed on credit institutions. Additionally, in the absence of a further breakdown of the types of financial institutions that were fined and the nature of breaches identified, it was not possible for the evaluation to make a judgement on the proportionality, effectiveness and dissuasiveness of the fines imposed. It is acknowledged, however, that financial institutions subject to FIU supervision are not subject to the Core Principles and are relatively small in terms of assets and turnover. The levels of fines imposed in those cases may have been appropriate.

*766.* No such sanctions have been imposed on directors or senior management for AML/CFT failures by financial institutions.

*Sanctions - statistics*

767. Statistics on sanctions are referred to in the preceding section. As already mentioned, the statistics provided were not broken down sufficiently to enable the evaluation team to make a conclusive judgement on the proportionality, effectiveness and dissuasiveness of the sanctions imposed.

*Market entry*

***Recommendation 23 (c. 23.3, c. 23.3.1, c. 23.5, c. 23.7, licensing/registration elements only)***

*Prevention of Criminals from Controlling Institutions, Fit and Proper Criteria (c. 23.3 & 23.3.1)*

768. Article 2(1) of the FSA Act provides that the FSA is responsible for monitoring and market entry of the credit and financial institutions which are subject to FSA supervision.

769. Section 3.10 of the 3rd round Mutual Evaluation Report sets out, at paragraphs 663 to 669, the assessors' analysis, which concludes that the FSA has the power to prevent, to a certain extent, criminals from infiltrating credit and financial institutions and may refuse to grant authorisation or revoke authorisation if the applicant, an institution or its managers have been punished for an

economic offence. However, while it appeared that criminals were able to be excluded in practice, the 3rd round assessors recommended that this power be made explicit in the legislation.

770. Since the 3rd round MER, further provisions have been introduced to impose conditions on those holding a qualifying interest in credit and financial institutions.

771. For instance, Art. 29 of the CrIA reads:

*"Requirements for persons acquiring and having a qualifying holding*

*A qualifying holding in a bank may be acquired, held and increased and control over a bank may be achieved, held and increased by any person conforming to the following requirements (hereinafter in this Article person):*
*1) who has an impeccable business reputation and is acting in the course of the acquisition according to the principles of sound and prudent management of a bank;*
*2) after the holding has been acquired or increased, is electing, naming or assigning the director of the bank to be only such a person who conforms to the requirements specified in Art. 48 of this Act;*
*3) whose financial situation is sufficiently strong to ensure the reliable and regular operation of the bank, and in case of a legal person its annual reports if such exist allow adequate assessment of its financial situation;*
*4) who is able to ensure that the bank is capable of following the prudential requirements specified in this Act, in case of a legal person primarily the requirement that the consolidation group a part of which the bank becomes has a structure that allows the exercise of sufficient supervision, exchange of information and co-operation between financial supervision authorities;*
*5) with respect to whom there is no justified suspicion that the acquisition, possession or increase of the holding or the control over the bank is connected to money laundering or terrorist financing or any attempts thereof or increases such risks. "*

772. Similar provisions are found in the various sectoral legislation, as follows:

- In investment firms – Art. 72 of the Securities Market Act
- In investment funds – Art. 44 of the Investment Funds Act
- In insurance service providers – Art. 60 of the Insurance Activities Act
- In payment service providers and e-money institutions – Art. 38 of the Payment Institutions and E-money Institutions Act.

773. All these provisions require persons holding qualifying interests in a financial institution to have an "impeccable business reputation" and require that such a holding will not increase money laundering or terrorist financing risk.

774. During the onsite visit it was confirmed that, in practice, assessing a person's business reputation involved checking criminal records both domestically and internationally and that a record of an economic offence would prevent a person from holding a qualifying interest.

775. In order to detect where a person holding the controlling interest is acting on behalf of somebody else, the FSA uses a personal declaration system. The FSA requires a written declaration from the beneficial owner, and includes warnings about a false declaration being grounds for criminal proceedings. The FSA also searches public databases and makes inquiries to the FIU and other Estonian and international authorities in order to verify information about the beneficial owner.

776. Similarly, new provisions have been introduced attaching fitness and propriety conditions to senior management positions in the various institutions supervised by the FSA. These are as follows:

- In credit institutions – Art. 56 of CrIA;
- In investment firms - Art. 79 of the Securities Market Act;
- In investment funds - Art. 51 of the Investment Funds Act;
- In insurance service providers - Art. 48 and Art. 138 (for insurance broker) of the Insurance Activities Act;
- In payment service providers and e-money institutions - Art. 47 of the Payment Institutions and E-money Institutions Act.

777. These provisions prohibit individuals who have been punished for an economic offence from holding senior positions and require appointees to have appropriate education, experience and professional qualifications.

778. Financial institutions supervised by the FIU are not subject to the Core Principles and are therefore dealt with under c. 23.7.

*Licensing or Registration of Value Transfer/Exchange Services (c. 23.5)*

779. Article 52 of the MLTFPA provides an obligation to register in the register of economic activities for (inter alia) providers of currency exchange services and providers of services of alternative means of payment[64].

780. Registration must occur before commencement of operations by the entity and involves the submission of a detailed application that includes information concerning the institution, its activities, its addresses, its directors and its beneficial owners.

781. Article 55 states that registration shall be refused if the directors or beneficial owners of the institution have committed specific crimes, including money laundering and terrorist financing, or "other intentionally committed criminal offence". Similarly, registration can be deleted if the offences occur following registration.

782. Payment Service providers are subject to the full licensing requirements by the FSA, including measures to prevent criminals from holding controlling interests or holding a management function and fit and proper criteria in relation to directors and senior management.

*Licensing of other Financial Institutions (c. 23.7)*

783. Article 52 of MLTFPA states that financial institutions who are not subject to supervision by the FSA pursuant to Art. 2 of the FSA Act; loan and savings associations; consumer credit providers; providers of services of alternative means of payment; pawnbrokers; and leasing companies; are required to register themselves in the register of economic activities before commencing operations in the corresponding area of activity. Since the adoption of the Payment Institutions and E-money Institutions Act, the FSA has become the licensing authority for payment service providers and electronic money institutions, which are not subject to the Core Principles (for details on the licensing procedure of these institutions see c. 23.3).

784. These institutions are obligated persons and are supervised by the FIU, pursuant to Art. 47 of MLTFPA. The supervisory powers and monitoring activities of the FIU, including sanctions imposed, are described in more detail under other parts of this section.

[64] Registration provisions were amended on 1 July 2014 which now provide for licensing.

***On-going supervision and monitoring***

***Recommendation 23 & 32 (c. 23.4, c. 23.6, c. 23.7, supervision/oversight elements only & c. 32.2d)***

*Application of Prudential Regulations to AML/CFT (c. 23.4)*

785. Regulatory and supervisory measures in relation to those institutions subject to Core Principles are applied consistently for prudential and AML/CFT purposes, including the assessment of risk and vulnerability patterns, assessment of management information systems, mechanisms of transaction monitoring and consolidated supervision.

786. On-site supervision is undertaken by the FSA in accordance with an annual on-site inspection programme. The selection of institutions for inspection is based on a number of risk factors, including the size of the institution, the type of business conducted and SAR reporting behaviour.

*Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6)*

787. Persons providing money or value transfer services (i.e. payments institutions) and persons providing money or currency exchange services are the obligated persons pursuant to the MLTFPA and are supervised for this purpose by the FSA or the FIU.

*Supervision of other Financial Institutions (c. 23.7)*

788. All financial institutions that are not mentioned in Criterion 23.4 are obligated persons pursuant to the MLTFPA and supervised by either the FSA or the FIU, depending on their specific activities.

789. Institutions that are not required to be licensed by the FSA are required to be registered on register of economic activities before commencing operations, in accordance with Art. 52 MLTFPA.

*Statistics on On-Site Examinations (c. 32.2(d), all supervisors)*

790. The following statistics have been provided by the FSA:

**Table 23: On-site/Off-site FSA supervision**

| **2009** | | | | | |
|---|---|---|---|---|---|
| | **Total number of entities in 2009** | **Number of on-site visits conducted** | **Number of AML/CFT specific (ad hoc) on-site visits conducted** | **Number of off-site examinations conducted** | **Number of AML/CFT combined actions with general supervision** |
| | **1** | **2** | **3** | **4** | **5** |
| **FINANCIAL SECTOR** | | | | | |
| Credit institutions | **7** | 1 | 1 | 14 | 0 |
| Branches of foreign credit institutions | **10** | 1 | 0 | 20 | 1 |
| Investment firms | **7** | 0 | 0 | 0 | 1 |
| Fund Management | **17** | 0 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| Companies | | | | | |
| Life Insurance | **5** | 0 | 0 | 0 | 0 |
| PSP-s | **N/A** | N/A | N/A | N/A | N/A |
| E-money SP | **N/A** | N/A | N/A | N/A | N/A |

| **2010** | | | | | |
|---|---|---|---|---|---|
| | **Total number of entities** | **Number of on-site visits conducted** | **Number of AML/CFT specific (ad hoc) on-site visits conducted** | **Number of off-site examinations conducted** | **Number of AML/CFT combined actions with general supervision** |
| | **1** | **2** | **3** | **4** | **5** |
| **FINANCIAL SECTOR** | | | | | |
| Credit institutions | **7** | 0 | 0 | 14 | 0 |
| Branches of foreign credit institutions | **11** | 0 | 2 | 22 | 0 |
| Investment firms | **8** | 1 | 3 | 0 | 0 |
| Fund Management Companies | **16** | 0 | 0 | 0 | 1 |
| Life Insurance | **5** | 1 | 0 | 4 | 0 |
| PSP-s | **N/A** | N/A | N/A | N/A | 6 |
| E-money SP | **N/A** | N/A | N/A | N/A | N/A |

| **2011** | | | | | |
|---|---|---|---|---|---|
| | **Total number of entities** | **Number of on-site visits conducted** | **Number of AML/CFT specific (ad hoc) on-site visits conducted** | **Number of off-site examinations conducted** | **Number of AML/CFT combined actions with general supervision** |
| | **1** | **2** | **3** | **4** | **5** |
| **FINANCIAL SECTOR** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Credit institutions | **7** | 1 | 1 | 3 | 2 |
| Branches of foreign credit institutions | **10** | 1 | 1 | 3 | 0 |
| Investment firms | **7** | 0 | 1 | 0 | 1 |
| Fund Management Companies | **17** | 0 | 0 | 0 | 1 |
| Life Insurance | **5** | 0 | 0 | 0 | 1 |
| PSP-s | **6** | 1 | 0 | 0 | 2 |
| E-money SP | **N/A** | N/A | N/A | N/A | N/A |

| **2012** | | | | | |
|---|---|---|---|---|---|
| | **Total number of entities** | **Number of on-site visits conducted** | **Number of AML/CFT specific (ad hoc) on-site visits conducted** | **Number of off-site examinations conducted** | **Number of AML/CFT combined actions with general supervision** |
| | **1** | **2** | **3** | **4** | **5** |
| **FINANCIAL SECTOR** | | | | | |
| Credit institutions | **8** | 0 | 4 | 3 | 0 |
| Branches of foreign credit institutions | **9** | 0 | 0 | 2 | 1 |
| Investment firms | **5** | 2 | 0 | 0 | 1 |
| Fund Management Companies | **18** | 0 | 0 | 0 | 0 |
| Life Insurance | **5** | 0 | 0 | 0 | 0 |
| PSP-s | **8** | 1 | 2 | 0 | 2 |
| E-money SP | **N/A** | N/A | N/A | N/A | N/A |

| 2013 | | | | | |
|---|---|---|---|---|---|
| | **Total number of entities** | **Number of on-site visits conducted** | **Number of AML/CFT specific (ad hoc) on-site visits conducted** | **Number of off-site examinations conducted** | **Number of AML/CFT combined actions with general supervision** |
| | **1** | **2** | **3** | **4** | **5** |
| **FINANCIAL SECTOR** | | | | | |
| Credit institutions | **8** | 0 | 5 | 7 | 0 |
| Branches of foreign credit institutions | **7** | 0 | 1 | 4 | 0 |
| Investment firms | **4** | 0 | 0 | 4 | 0 |
| Fund Management Companies | **18** | 0 | 0 | 18 | 2 |
| Life Insurance | **4** | 0 | 0 | 0 | 0 |
| PSP-s | **10** | 1 | 3 | 0 | 2 |
| E-money SP | **N/A** | N/A | N/A | N/A | N/A |

**Table 24: FIU On-site inspections**

| | **Total number of entities** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| **Financial institutions** | 316 | 82 | 15 | 7 | 6 | 11 |
| **Credit institutions** | 17 | 0 | 6 | 0 | 0 | 0 |

*Statistics on Formal Requests for Assistance (c. 32.2(d), all supervisors)*

791. Estonia does not keep statistics on requests for assistance made or received by supervisors. Information provided by the FSA is that "in recent years" the number of requests made by the FSA has been "around 15" and the number of the requests received from foreign authorities has been "around 25". Information provided by the FIU is that it has received requests for information from 2 overseas Central Banks and one overseas Ministry of Finance.

*792.* It is unclear whether there have been any refusals to provide assistance and, if so, on what grounds these requests were refused.

***Effectiveness and efficiency (market entry [c. 23.3, c. 23.3.1, c. 23.5, c. 23.7]; on-going supervision and monitoring [c. 23.4, c. 23.6, c. 23.7], c. 32.2d]***

793. Since the last MER, the Estonian Authorities have introduced sufficient legal and regulatory arrangements to prevent criminals from owning or operating financial institutions supervised by the FSA. Although the Estonian authorities do not maintain statistics of cases where fitness and propriety criteria have been applied in practice to bar individuals from ownership or management of financial institutions, this information can be manually retrieved. The authorities referred to a number of cases where this has happened – once in 2011, twice in 2012, once in 2013.

794. Licensing and registration undertaken by the FIU (which only deals with financial institutions which are not subject to Core Principles) involves FIU staff reviewing detailed information concerning the relevant institution, its activities, its directors and its beneficial owners. Such review occurs upon application.

795. Regarding on-going supervision and monitoring, the FSA utilises a comprehensive risk based model to determine its AML/CFT supervisory priorities and to plan relevant actions, including an annual AML/CFT on-site inspection programme. More information about the FSA's on-site and off-site processes is detailed above under the effectiveness section of Recommendation 29.

796. The FSA provided statistics on the number of on-site and off-site inspections conducted by the FSA (see Table 23). In the table, the second column represents the number of full scope AML/CFT on-site inspections, while the third column represents the number of ad-hoc AML on-site inspection focussed on one or more particular aspects of AML/CFT requirements. Column 4 refers to the number of AML/CFT off-site inspections, which includes receipt and analysis of relevant policies, procedures and controls. In addition, column 5 represents combined supervisory action which is undertaken by non-AML supervisory teams for prudential purposes but which, because of the nature of the information reviewed or inspected, may have relevance in an AML/CFT context and the results of which are shared with the AML/CFT supervisory team. The FSA did not indicate which of the combined actions were in fact on-site inspections.

797. With respect to credit institutions, the supervisory actions undertaken by the FSA were as follows:

| | | | | |
|---|---|---|---|---|
| 2009: | 7 credit institutions | 2 on-sites | 14 off-site | 0 combined actions |
| 2010: | 7 credit institutions | 0 on-sites | 14 off-site | 0 combined actions |
| 2011: | 7 credit institutions | 2 on-sites | 3 off-site | 2 combined actions |
| 2012: | 8 credit institutions | 4 on-sites | 3 off-site | 0 combined actions |
| 2013: | 8 credit institutions | 5 on-sites | 7 off-site | 0 combined actions |

798. With respect to branches of credit institutions, the supervisory actions undertaken by the FSA were as follows:

| | | | | |
|---|---|---|---|---|
| 2009: | 10 branches | 1 on-site | 20 off-site | 1 combined action |
| 2010: | 11 branches | 2 on-sites | 22 off-site | 0 combined actions |
| 2011: | 10 branches | 2 on-sites | 3 off-site | 0 combined actions |
| 2012: | 9 branches | 0 on-sites | 2 off-site | 1 combined action |
| 2013: | 7 branches | 1 on-site | 4 off-site | 0 combined actions |

799. The figures indicate that in the 5 year period under review, the 7 credit institutions (8 after 2012) were subject to 13 AML/CFT on-site inspections, 41 off-site measures and 2 other supervisory

actions. For the same period, 9 (average) branches of foreign credit institutions were subject to 6 AML/CFT on-site inspections, 51 off-site measures and 2 other supervisory actions. It is to be noted that 2 credit institutions and 2 branches of overseas credit institutions effectively hold 89% of the market share in Estonia. According to the FSA's risk based approach to supervision, these receive the highest attention. It is therefore the view of the evaluation team that credit institutions and branches of foreign credit institutions are subject to sufficient ongoing supervision and monitoring.

800. With respect to the remaining financial institutions, the FSA pointed out that fund management companies, which comprise a significant proportion of financial institutions, operate via and outsource their AML/CFT functions to credit institutions. Their compliance with AML/CFT obligations is thus supervised by way of FSA interaction with the credit institutions themselves. The on-site visits conducted at credit institutions (which are referred to in the preceding paragraphs) would include fund management companies' AML/CFT compliance.

801. The numbers of on-sites for the remaining financial institutions (investment firms, life insurance, payment service providers and e-money institutions) are as follows:

| | | | | |
|---|---|---|---|---|
| 2009: | 12 financial institutions | 0 on-sites | 0 off-site | 1 combined action |
| 2010: | 13 financial institutions | 5 on-sites | 4 off-site | 6 combined actions |
| 2011: | 18 financial institutions | 2 on-sites | 0 off-site | 4 combined actions |
| 2012: | 18 financial institutions | 5 on-sites | 0 off-site | 3 combined actions |
| 2013: | 18 financial institutions | 4 on-sites | 4 off-site | 2 combined actions |

802. The FSA indicated that according to its risk assessment, the number of on-site inspections is considered adequate. However, an analysis of the figures (without consideration of the concrete risk) indicates that over the 5 year period under review there were (on average) 16 financial institutions which were subject to 16 AML/CFT on-sites. This translates into one on-site visit every five years for the financial sector covering the financial institutions mentioned above. Notwithstanding the fact that these institutions collectively account for a small share of the financial market, the evaluation team does not consider that the number of on-site visits is sufficient, especially since the total number of off-site actions is limited to 8. In particular, it was noted that out of 5 life insurance companies (4 in 2013) only one company received an on-site inspection in the period under review. It is to be noted however that 16 AML/CFT supervisory actions were undertaken within the general supervisory framework of the FSA.

803. The FIU indicated that it has undertaken the following supervisory actions with respect to financial institutions.

| | **2009** | **2010** | **2011** | **2012** |
|---|---|---|---|---|
| **Financial institutions** | 82 | 15 | 7 | 6 |
| **Credit institutions** | 0 | 6 | 0 | 0 |

804. No further breakdown was provided by the FIU. The number of inspections undertaken by the FIU has decreased markedly over time. This is a reflection of the FIUs supervisory programme which focuses on awareness raising and targeting individual entities, rather than ongoing compliance monitoring. Overall, the number of inspections does not appear satisfactory.

**Guidelines**

**Recommendation 25 (c.25.1 – guidance for financial institutions other than feedback on STRs)**

*Summary of 2008 factors underlying the rating*

805. Recommendation 25 was rated PC in the 3rd round report for the following shortcomings:

- The guidelines issued by the FSA were out of date;
- The FIU had not issued guidelines explaining the legal requirements and preventive measures to supervised entities.

806. The FSA is empowered by Art. 57 of the FSA Act to issue advisory guidelines to explain legislation regulating the activities of supervised entities.

807. The FSA issued the guideline "Additional measures for prevention of money laundering and terrorist financing in credit and financial institutions" in October 2008 and has published it on the web-site of the FSA. This provides guidance on the application of AML measures by financial institutions suggests best practise in relation to AML compliance obligations, including transaction monitoring, training, CDD, implementation of the risk-based approach, and reporting of suspicions. It does not, however, contain guidance in relation to ML/FT techniques and methods.

808. The FSA also issued a renewed guideline "Measures for preventing of money laundering and terrorist financing in credit and financial institutions" in July 2013. This does not take effect until Jan 2014. This guidance updates and expands upon the previous guidance, providing suitable information and guidance on the application of AML measures and compliance with AML obligations. It does not contain any information or guidance in relation to ML/FT techniques and methods.

809. The FIU is empowered by Art. 39 of the MLTFPA to issue advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing.

810. The FIU has issued the following guidelines in order to assist the entities it supervises:

- auditors and providers of accounting services:
- traders:
- pawn houses;
- casinos:
- notaries public (in cooperation with Chamber of Notaries)

***Effectiveness and efficiency (R. 25)***

811. Financial institutions who were interviewed during the onsite visit confirmed that guidance from the Estonian authorities was useful and effective. Compliance staff confirmed that they had incorporated the guidelines into their own internal processes and procedures and had referred to this material as part of their internal training delivered to staff.

812. Institutions all suggested that the information on the authorities' websites was a valuable resource for obliged persons.

3.7.2 Recommendations and comments

***Recommendation 23***

813. There is a dedicated supervisor for the required range of financial institutions, with sufficient statutory powers to enable the effective supervision of compliance with AML/CFT requirements.

The FSA's risk model for supervision, as described by the authorities, is comprehensive and its application appears to be yielding appropriate results.

814. Since the last MER, the Estonian Authorities have introduced sufficient legal and regulatory arrangements to prevent criminals from owning or operating financial institution supervised by the FSA. However, the authorities should consider amending the wording of Art. 48(3) to ensure that supervisors have access to all records, documents or information relevant to monitoring compliance, including all documents or information related to accounts or other business relationships, or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions.

815. Directors and managers of financial institutions subject to Core Principles are also subject to fit and proper tests, including assessment of expertise and integrity.

816. All financial institutions, including money or value transfer/exchange services, are registered and subject to AML/CFT supervision.

817. Nevertheless, the FSA should consider, as appropriate, undertaking more supervisory action on life insurance companies, investment firms and payment service providers.

818. The Estonian authorities should also review the staffing levels at the FIU to ensure that sufficient supervisory staff are in place to effectively cover the full range of entities supervised for compliance with AML/CFT obligations, including increasing the number of on-site inspections. The FIU should introduce a proper internal methodology for supervisory purposes to ensure that on-site inspections are conducted in a systematic manner.

***Recommendation 17***

819. While there are authorities empowered to apply sanctions, the Estonian Authorities should review the sanctioning provisions in the MLTFPA and the various sectoral legislation, in order to provide for consistent application of sanctions across all financial institutions.

820. The Estonian authorities should review the range of financial penalties available, to ensure that they are sufficiently proportionate, dissuasive and effective.

821. The Estonian authorities should extend the power to apply sanctions to directors and senior managers of financial institutions.

822. The Estonian authorities should use a wider range of sanctions, financial penalties and sanctions against individuals where appropriate.

823. Sanctions imposed by the FSA and the FIU should be published, where appropriate.

***Recommendation 29***

824. Powers to monitor compliance are broadly adequate, including the power to compel records and conduct inspections.

825. Estonian Authorities should consider reviewing the use of supervisory powers in the MLTFPA and the various sectoral legislation, in order to provide for consistent application of supervision across all financial institutions. In particular they should consider amending Art. 48 of MLTFPA to include the wider application of powers that is contained in the sectoral legislation.

826. The Estonian authorities should introduce a power to apply sanctions to directors and senior managers of financial institutions.

***Recommendation 30 (all supervisory authorities)***

Staffing, training and structure of the FSA is broadly appropriate. While training and professional standards at the FIU are appropriate, it is not clear that there are sufficient supervision staff at the FIU to adequately supervise the financial institutions for which they are responsible.

***Recommendation 32***

827. The authorities should collect statistics on formal requests for assistance made or received by supervisors, including whether such requests were granted or refused.

828. The FIU should maintain statistics on on-site inspections broken down by category of financial institution.

3.7.3 Compliance with Recommendations 23, 29, 17 & 25

| | Rating | Summary of factors relevant to s.3.10. underlying overall rating |
|---|---|---|
| **R.17** | **PC** | • Range of available sanctions is neither effective nor proportionate for certain categories of financial institutions;<br>• Maximum financial penalties do not appear dissuasive;<br>• Sanctions available for legal persons that are financial institutions are not available for their directors and senior management;<br>**Effectiveness**<br>• Narrow range of sanctions applied in practice. |
| **R.23** | **LC** | **Effectiveness**<br>• Insufficient ongoing supervision and monitoring of investment firms, life insurance companies and payment service providers;<br>• Effectiveness issues for the FIU - low number of staff, low levels of on-site inspections, decreasing levels of off-site supervision, no proper internal methodology for conducting on-site inspections. |
| **R.25** | **C** | |
| **R.29** | **LC** | • No adequate sanctioning power against directors and senior management for breaches by a financial institution. |

# 4. PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS

General

829. All FATF designated non-financial businesses and professions are subject to the provisions of the MLTFPA[65] (see Table 5). The application of preventive measures has been extended to cover other business and professions which may be abused for money laundering or terrorist financing purposes, such as for instance, traders other than those dealing in precious metals and stones, auditors, and non-profit associations and foundations.

830. Article 3 of the MLTFPA provides the list of DNFBPs that are considered as obliged entities:

a) organisers of games of chance;

b) persons who carry out or act as intermediaries in transactions with real property;

c) traders for the purposes of the Trading Act, if a cash payment of more than 15,000 euros or an equal amount in another currency is made to the trader, regardless of whether the financial obligation is performed in the transaction, in a lump sum or in several related payments, unless otherwise provided by law;

d) pawnbrokers;

e) persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes;

f) auditors and providers of accounting services;

g) providers of accounting or tax advice services;

h) providers of trust[66] and company services;

i) non-profit associations and foundations for the purposes of the Non-profit Associations and Foundations Act, if a cash payment of more than 15,000 euros or an equal amount in another currency is made to them, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments, unless otherwise provided by law;

j) notaries public, attorneys, enforcement officers, bankruptcy trustees, interim bankruptcy trustees and providers of other legal services if

- they act in the name and on account of a customer in financial or real property transactions,
- they guide planning or entry into a transaction or perform a professional operation or provide a professional service, which involves the following:
  - the purchase or sale of immovables, enterprises or shares of companies;
  - the management of the customer's money, securities or other property;
  - the opening or managing of bank accounts or security accounts;
  - the acquisition of funds necessary for the foundation, operation or management of companies;

[65] Although trust service providers are listed as obligated entities under the MLTFPA, there are no such entities operating in Estonia.

[66] Although trust service providers are listed as obligated entities under the MLTFPA, there are no such entities operating in Estonia.

- the foundation, operation or management of trusts, companies or other similar entities.

831. Persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones and NPOs were made subject to the provisions of the MLTFPA (MLTFPA Art. 3(1) $6^1$) by an amendment to the MLTFPA, which entered into force on 18th May 2012.

832. Dealers in precious metals and stones are covered by Art. 3 e) (for buying-in and wholesale) and Art. 3 c) (for retailers). For the purposes of the MLTFPA, 'precious stones' means natural and artificial precious stones and semi-precious stones, their powder and dust, and natural and cultivated pearls. The terms 'precious metal' and 'precious metal articles' under the MLTFPA have the same meaning as that set out in the Precious Metal Articles Act (Art. 3 (4) of the MLTFPA). Article 2 of the Precious Metal Articles Act determines that "precious metal" means pure gold, silver, platinum and palladium and their alloys. "Article of precious metal" means an object which is wholly or partially manufactured from one or several precious metals with at least the minimum standard of fineness as permitted in Art. (4)2) and ($2^1$) of this Act.

833. The Precious Metal Articles Act stipulates that an undertaking entered in the commercial register or the register of taxable persons concerning which a registration has been made in the Register of Economic Activities, which provides the right to engage in the manufacture or import of or wholesale trade or retail trade in articles of precious metal may manufacture, offer for sale on a wholesale or retail basis or transfer for a charge and import articles of precious metal. Upon the importing of and wholesale trade in articles of precious metal, if the transaction value exceeds 960 euros, payment for articles of precious metal is made by way of a non-cash settlement.

834. According to Art. 52(1)7) of the MLTFPA, persons engaged in the buying-in[67] or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes are required to register in the Register Of Economic Activities before commencing operations in the corresponding area of activity. The FIU risk analyses/practice indicated that there are high risks in this sector and therefore the authorities decided to mitigate those risks going beyond the FATF Recommendations. This issue was also discussed in Governmental Committee meeting before actions were taken (the relevant amendments to MLTFPA were drafted).

835. All DNFBPs are subject to the same CDD and record keeping requirements as financial institutions. The findings under Section 3 of the MER, as well as the deficiencies identified under Recommendations 5 to 11 for financial institutions are also applicable to DNFBPs (for details see Section 3 of the MER). The following sections only deal with sector-specific issues.

### 4.1. Customer due diligence and record-keeping (R.12)

(Applying R.5, R.8, R.10 and R.11)

836. As described in the 3rd round report, Estonia was rated "Partially Compliant" for Recommendation 12.

837. The factors underlying the 3rd round rating were the following:

- The same concerns in the implementation of Recommendations 5, 6, 8—11 apply equally to DNFPB.

[67]The buying-in means the buying of items from the market, usually from natural persons in small quantities and with bargainable prices. The *modus operandi* includes the advertisement where people (general public) is invited to bring their precious metal items (like old golden teeth, broken jewellery etc) and exchange these to cash. The purpose of the law is to regulate precious metal articles that are of interest to the consumers for personal use and/or investment.

- There are no Regulations/Directives to DNFBP laying down requirements for internal control procedures for managing AML/CFT risks.
- Though DNFBP are required under Art. 19(2) MLTFPA to apply enhanced due diligence procedures for business relationships or transaction with non-face-to-face customers, no guidance is provided as to the possible enhanced due diligence measures that DNFPB should take to mitigate the risks for non-face-to face relationships and transactions.
- Casinos are required to identify but not verify the name of a client who pays or receives in a single transaction or several related transactions over a designated amount.

4.1.1 Description and analysis

838. Estonia has taken steps to comply with the FATF standards and the MONEYVAL recommendations. The FIU has published guidelines on its website and organised trainings in order to improve awareness in the non-financial sector.

839. The requirements in the MLTFPA apply in the same manner for both the financial sector and the DNFBPs. However, some specific CDD provisions apply exclusively to DNFBPs (as explained in more detail in this section). For instance, a notary public, enforcement officer, bankruptcy trustee, auditor, attorney and another legal service provider may identify and verify the identity of a customer or a person participating in a transaction and a beneficial owner in the course of establishing a business relationship or entering into a transaction, provided that it is necessary for the purpose of not interrupting the ordinary course of professional activities and if the risk of financing money laundering or terrorist financing is low. However, in these cases the application of due diligence measures must be completed as soon as possible after the first contact and before performing any binding acts.

840. The risk-based approach was introduced in the MLTFPA and according to Art. 14(3) all obligated person shall take all CDD measures but may choose the appropriate scope of application based on the nature of the business relationship or transactions or the risk level of the person or customer. Some guidelines were issued by the FIU to assist some sectors (including the management of risks). The FIU issued and published guidelines based on Art. 39(1) of the MLTFPA for traders, auditors and providers of accounting services, pawn brokers, casinos and notaries public. .

841. According to Art. 29 an obligated person shall establish written rules of procedure for the application of CDD measures including the assessment and management of ML/FT risks and collection and preservation of data. Competent authorities control the existence and content of internal rules during the onsite visit. Failure to apply internal security measures is punishable by a fine. These obligations do not apply to non-profit associations or foundations.

842. Based on Art. 30 of the MLTFPA all obligated entities are required to establish rules of procedures which correspond to the type, scope and complexity of the professional activities of the entity. Rules of procedure shall describe low and high risk level, including risks arising from means of communication, computer network and other new technological development as well as establish the appropriate procedures for CDD and preservation of data and documents.

843. The FIU published a guidance paper on the CDD measures applicable in non-face-to-face relationships and transactions. During the onsite visit all the representatives of DNFBPs confirmed that they usually meet the customer in person (except for online casinos which have specified requirements) before establishing a business relationship.

844. There are no Regulations to DNFBPs laying down requirements for internal control procedures, including the managing AML/CFT risks. The scope of the Minister Regulation No. 10

does not cover DNFBPs based on Art. 30 of the MLTFPA. The Estonian authorities stated that sector specific guidelines could facilitate the improvement of effectiveness and awareness raising and not the Regulation as DNFBPs are not homogeneous and their activities are very different. Comprehensive advisory measures for managing AML/CFT risks were set out in advisory guidelines issued by FIU, the Chamber of Notaries and the Estonian Bar Association which are considered to be very useful according to the representatives of the sectors met onsite. In the view of these evaluators the guidelines include the necessary provisions.

***Recommendation 12 (rated PC in the 3rd round report)***

*Applying Recommendation 5(c.12.1)*

*Casinos (Internet casinos / Land based casinos)*

845. Organisers of games of chance (including casinos and internet casinos) fall under the scope of MLTFPA. According to Art. 3 of the Gambling Act games of chance are defined as '*games, the outcome of which depends on chance and which are played by means of a mechanical or electronic device or by mediation of the organiser of the game'*. According to Art. 5 of the Gambling Act, remote gambling is '*the organisation of gambling in a manner where the outcome of the game is determined by an electronic device and the player can participate in the game by electronic means of communication, including telephone, internet and media services'*.

846. As determined in Art. 16 of the MLTFPA, an organiser of games of chance shall identify and verify the data specified in subsection 23(3) regarding all persons who pay or receive in a single transaction or several related transactions an amount exceeding 2,000 euros or an equal amount in another currency. On the basis of this requirement, the obligated person shall register the address of the place of residence and the profession or the area of activity of the player and determine whether the player is a PEP. Article 16 does not make reference to Art. 23(1) and (2) which provide for the requirement to register data and copies of documents for identification and verification. However, with the coming into force of the new Gambling Act on 1 January 2009, all customers, regardless of the amount of the financial transactions, have to be identified and the information verified and registered before entering a gambling venue. As stated in Art. 37(10) of the Gambling Act, "*before a person enters a gaming location for games of chance, the organiser of the games of chance shall verify the data in the electronically maintained database regarding the persons who have visited the gaming location for games of chance on the basis of the identification document presented for identification and shall register the time and date of the person's arrival in the gaming location for games of chance in the database*."

847. According to Art. 30 of MLTFPA the obligated persons are required to set the rules and procedures for the application of CDD measures and determining risk factors as regards the customer.

848. The representatives of organisers of games of chance (including online casinos) confirmed that whenever the amount of a transaction or a series of connected transactions exceeds 2,000 EUR, the client is identified and verified as determined in the MLTFPA. Some of them stated that identification and verification is also possible at gaming tables, or when paying or receiving cash in exchange of chips.

849. The evaluation team was informed that as a general requirement, the registration of winnings and pay-outs has to be performed in all cases, regardless of the additional CDD measures that have to be applied according to the MLTFPA to all persons who pay or receive in a single transaction or several linked transactions an amount exceeding 2,000 euro or an equal amount in another currency.

850. According to 53 of the Gambling Act the gambling operator is required to apply measures to avoid providing any gambling opportunities to persons who are younger than the age set out in this

Act and who play by remote gambling in Estonia; the identification of every player; the registration of every player's identification data, and the time and date of entering and exiting the gaming environment; the keeping of record of the bets made by every player, payments transferred to the account of the gambling operator for the making of bets, refunds made and prizes distributed to players; the acceptance of bets and payments transferred to the account of the gambling operator for the making of bets only from the settlement account of the same player or from a player in the gaming location of the same gambling operator; the making of distributions only to the same settlement account, from which the player has transferred a payment to the account of the gambling operator for the making of bets in gambling; an unrestricted access for supervisory officials to the gaming equipment.

851. Article 58 of the Gambling Act requires operators to implement an electronic recordkeeping and control system. A gaming table is connected with the electronic recordkeeping and control system if settlements are performed at the gaming table or if the game is fully or partially organised by electronic means. The data recorded in the electronic recordkeeping and control system is stored for at least five years. As a general rule gaming machines are programmed not to give out more than 2,000 euros in cash.

852. The representatives of the casinos informed the evaluators that when CDD is applied in case the amount of a transaction or a series of connected transactions exceeds 2,000 EUR (in most of the cases when chips are paid back), that information is checked against the identification information registered at the entrance of the casino.

Implementation

853. The representatives of casinos interviewed onsite were knowledgeable of their CDD requirements. They indicated that the requirement to identify and verify a player whenever the EUR 2,000 threshold is exceeded does not pose any undue difficulties in practice. When entering the casino, customers are required to sign a consent form which enables the casino to request all documentation necessary to fulfil its CDD requirements. Customers are also required to sign a written statement confirming the validity of the documentation provided. Information is verified from independent reliable sources.

854. The Estonian FIU issued guidelines to organisers of games of chance which lay down specific rules on the identification-verification procedure. An advisory guideline for remote gambling service providers has also been published and is available on-line. http://www.politsei.ee/dotAsset/201749.pdf and http://www.politsei.ee/dotAsset/201457.pdf

855. From the responses provided during the onsite visit casinos and online gambling providers appeared to have satisfactory identification and verification procedures and stringent internal controls in place. However, it remains unclear whether the risk based approach is used in practice and to what extent the CDD requirements are applicable for these service providers. In practice casinos appear to retain the same data and use the same procedures in the case of all clients. In view of the representatives, as gambling is generally considered to be a risky sector, high awareness is needed in their everyday procedures. As regards remote gambling, the operators seemed to have proper knowledge of requirements and they have appropriate procedures for the verification of data.

856. The evaluators were informed by at least one representative met on-site that transactions in land based casinos cover the purchase of chips in cash or credit card and pay out of winnings mainly via wire transfer to the customer's bank account. A certificate of winnings is supplied to the customer. The source of funds of the customer is not registered, not even in case of PEPs or high risk customers. The representatives could not confirm that there is a legal requirement on that.

857. The identification and verification of players is based on the identification documents submitted by the player, the completed and signed customer's questionnaire and information from

independent reliable sources: registers in case of Estonian citizens, available Estonian public registers and the internet. The source of funds is not registered. In case of bigger amount of payments or losses, casinos check whether the information on the customer is in line with the risk profile of a regular player (if relevant).

858. The representatives of remote gambling operators informed the evaluators that in most of the cases the player must register in person. Identification data is verified from documents provided, also on independent and reliable sources or from partner operators of the Gambling Association, furthermore the potential player needs to verify the residence as well as if he or she is the rightful owner of the money in the account.

859. The representatives of the casinos and online gambling services expressed the view that the highest risk scenarios within the context of a casino are PEPs, higher bets, and the type of the game or if the player requires getting the winning in cash. They also confirmed on mitigating and determining risks and risk based approach in their internal procedures.

*Real estate agents*

860. As regards real estate agents there are no further sector specific provisions determined in the MLTFPA. Legal requirements for CDD measures and record keeping are in place.

861. Since both the purchaser and the vendor are considered customers of the real estate agent, they both have to be subject to CDD requirements.

Implementation

862. Based on the information gathered during the interview with representatives of the sector, it appeared that CDD measures are not being fully applied in practice. Awareness as regards CDD and record keeping requirements seem to be very low. The evaluators were informed that in practice, the real estate agents do not enter into cash transactions, since cash is deposited with the notaries, who represent the client in financial or real estate transactions and also conduct CDD measures. Purchase and sale of real estate in Estonia must always include the services of a notary. In the view of the representatives of the sector, there is no further added value to require real estate agents to conduct CDD measures since these are already being applied by notaries. Real estate agents do not have registered data of the customers.

863. Efforts have been made by the FIU to reach out to the real estate agent sector by preparing training sessions and raising awareness during onsite visits. The evaluators are not aware of any guidelines for the sector prepared by the FIU.

*Dealers in precious metals and dealers in precious stones*

864. Dealers in precious metals and stones fall under the scope of MLTFPA under Art. 3($6^1$) (for buying-in and wholesale) and Art. 3(5) (for retailers). Persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones are required to apply all the CDD requirements irrespective of any threshold or limit. Traders (including retail traders in precious metals and stones) are only subject to CDD requirements where a cash payment of more than 15,000 euros or an equal amount in another currency is made, regardless of whether the financial obligation is performed in a lump sum or in several related payments.

*865.* Article 3(1)5) of the MLTFPA refers to the definition of a trader under Art. 2 of the Trading Act, which states that a "*trader is a person or body which, within the framework of the economic or professional activities thereof, offers and sells goods or offers and provides services".*

866. Whereas the persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones are required to register in the register of economic activities before commencing operations according to Art. 52(1)7) of the MLTFPA, the manufacturers and

importers of precious metals have to register their retail-sales according to the Precious Metals Act Art. 3. As of 1st September 2013, there were 121 registered persons dealing with precious metals.

867. The FIU informed the evaluation team that a growing trend has been identified in the handling, including trade, of large quantities of used articles of precious metal (incl. crushed items of gold) and gold granules of unknown origin since the second half of 2010. This knowledge was based on strategic and operational (case) analysis by the FIU. The issue has been addressed in several occasions with different counterparts, including Governmental Committee. The FIU has concluded that some of this gold may have been obtained as a result of crime or bought in via unlawful buying-in centres in different countries and has decided to take efforts in order to reduce and minimize the risks of ML. It has resulted to criminal investigation of cases and also it has initiated changes to tax regulations. Modifications in VAT related legislation have been made in several steps.

868. Items of gold obtained as a result of burglary and robbery are qualified as 'scrap gold' but in a different way as it is determined within the exceptions of the Precious Metal Articles Act (waste containing precious metals generated upon manufacturing). In practice, the Precious Metal Articles Act is interpreted in such a manner that the 'unusability' of gold is derived via the sale of crushed articles of precious metal for the purpose of their conversion into investment gold (for other manufacturing or melting). The MLTFPA stipulates that pawnbrokers are obliged to identify each client, including when items of gold are brought to the pawn shop. Entrepreneurs that participate in the scrap gold scheme only had to identify their clients when they sell gold to a value of at least 15,000 euros and were paid for the gold in cash. This situation also damaged the trustworthiness and reputation of the entrepreneurs who operate in this sector in accordance with law. Establishing obligations for entrepreneurs engaged in the buying-in and wholesale of precious metal that are similar to the obligations of pawnbrokers guarantees that entrepreneurs operating in similar areas of activity are treated in a similar manner in the context of the MLTFPA.

Implementation

869. The high value traders met on-site were to some extent aware that the requirements of the MLTFPA must be fulfilled if a cash payment of more than 15,000 EUR (in euros or currency) is made to the trader in one transaction or in several transactions which are linked. However, it was stated that cash transactions are not so common in everyday practice. Most transactions are carried out electronically. Identification data is verified and registered. In case of Estonian customers they are verified based on the Commercial Register, in case of non-residents on the submitted documents. The source of funds was not confirmed to be registered, not even in the case of PEPs. Cash transactions and customers from neighbouring countries are considered to pose a higher risk of ML.

870. The FIU has published guidelines for the sector on the implementation of CDD requirements and also on some defined cases which are considered to be higher risk and should be taken into consideration when applying CDD measures.

871. The evaluators noted a lack of appropriate understanding of certain CDD measures by this sector (especially the identification and verification of the beneficial owner and source of funds).

*Lawyers, notaries and other independent legal professionals and accountants*

872. Pursuant to Art. 3(2)) of the MLTFPA, CDD requirements apply to notaries public, attorneys, enforcement officers, bankruptcy trustees, interim bankruptcy trustees and providers of other legal services if they act in the name and on account of a customer in financial or real estate property transactions and if they guide the planning or entry into a transaction or perform a professional operation or provide professional services, which involve the following:

- The purchase or sale of immoveables, enterprises or shares of companies;

- The management of the customer's money, securities or other property;
- The opening or managing of bank accounts or security accounts;
- The acquisition of funds necessary for the foundation, operation or management of companies;
- The foundation, operation or management of trusts, companies or other similar entities.

873. All the activities of auditors and providers of accounting services are subject to the MLTFPA (Art. 3(1)7)).

874. Article 16(3) provides an exception to the requirement to verify the identity of the customer before or during the course of establishing a business relationship. A notary public, enforcement officer, trustee in bankruptcy, auditor, attorney or another legal service provider may identify and verify the identity of a customer or a person participating in a transaction and a beneficial owner while establishing a business relationship or entering into a transaction, provided that it is necessary for the purpose of not interrupting the ordinary course of professional activities and if the risk of money laundering or terrorist financing is low. The application of due diligence measures must be completed as soon as possible after the first contact and before performing any binding acts (Art. 16(3) and (4) of the MLTFPA). The authorities pointed out that this exception is not widely used.

875. The identification of persons and application of other due diligence measures by a *notary public* shall also be based on the Notarisation Act and the Notaries Act with the specifications provided by this Act.

876. According to the Notarisation Act, the personal data of a party which the notary indicates in a notarial deed shall be so detailed as to preclude doubt or confusion. A notary shall indicate in which manner he or she identifies a party. If the notary knows the party personally, he or she shall indicate the fact in the notarial deed. In the absence of an identity document, the notary shall identify a party under 15 years of age on the basis of state issued documents proving birth and filiation and the statements of the guardian and shall indicate it in the notarial deed.

877. If a notary cannot identify a person or doubts the identity of a person, but certification of a transaction is requested regardless of that, the notary shall indicate such fact in the notarial deed. A notary shall indicate the grounds of the right of representation and explain how he or she has established it in the notarial deed. If the notary cannot establish the necessary right of representation or doubts the right of representation, but certification is requested regardless of that, the notary shall indicate such fact in the notarial deed. In this case a notary may issue copies of notarial deeds only after the necessary identification of persons or establishment of the right of representation or disposal by the notary and the documents submitted for identification or establishment of the right of representation or disposal together with the original of the notarial deed.

878. According to Art. 44 of the Notaries Act determines that the electronic information system of notaries (E-Notary) shall contain digital notarial archives and books concerning the professional activities of a notary and may contain other functions necessary for the activities of a notary. The documents, including the source documents of notarial acts and books concerning the professional activities of a notary, prepared by a notary or substitute notary upon the performance of notarial acts and preserved pursuant to law belong to the state and shall be preserved in digital notarial archives.

879. In the electronic notary, notaries shall have access to the data recorded by them. Notaries may also verify data recorded by other notaries if notarial deeds prepared or notarial notations made by the other notaries are submitted to them as bases for acts of attestation.

880. According to Art. 44(3) of the Notaries Act, the Chamber of Notaries has the right to issue specifying instructions which are binding on notaries in accordance with this Act and other legislation, eg. concerning compliance with the diligence measures and rules of procedure provided for in the MLTFPA.

881. "*Instructions for Establishment of Rules of Procedure for the Application of Due Diligence measures provided for in Money Laundering and Terrorist Financing Prevention Act and International Sanctions Act* (ISA) *and of Internal Rules for auditing Compliance therewith*" were approved and published by the Chamber of Notaries in 2008. The Rules of Procedure establish an obligation to apply CDD measures at least upon performance of the notarial acts (professional operations) or provision of professional services under the scope of the MLTFPA. In March 2010, at the annual meeting of the Chamber of Notaries, a new version of guidelines was adopted, which establishes the rules of procedure for the due diligence measures enacted in MLTFPA and ISA, as well the rules of internal procedure for checking the implementation of the measures. At the beginning of 2010 and 2011 AML aspects were discussed at training for notaries and for employees of the notarial offices. In addition to the general training organised by the Chamber, several training have been conducted at notary offices to the employees of the notary. During on-site visits conducted by the Chamber, the implementation of MLTFPA and the guideline issued by the Chamber is inspected. Also information requests made by notaries through E-notary database which are required by law are always monitored.

882. Annex No.1 to these Instructions includes sample Rules of Procedure for the application of the due diligence measures provided for in the MLTFPA.

883. According to the sample Rules of Procedure of Instructions any information obtained upon application of the due diligence measures must be recorded in a corresponding written statement of the party to the notarial act or use of professional service (Appendix 1, 2 to Annex 1 of the Instructions), or the details must be indicated in the notarial deed or included in the data stored in the E-Notary electronic database.

884. Sample Rules of Procedure includes the obligation to apply due diligence measures from the moment of preparation for the notarial acts or professional services. Requirements of risk based approach are also reflected. CDD must be applied proportionately based on the nature of the notarial act or professional service and the persons involved in it or the extent of the risk for ML and TF. The requirements of enhanced CDD procedures are also covered and high-risk transactions are determined.

885. Beneficial owner information must be identified:

- in the case of a legal person registered in Estonia, on the basis of a detailed inquiry concerning the current general and personal data to the central database of the courts registration departments,
- the case of a company which shares are registered in the Estonian Central Register of Securities, on the basis of the electronic database of the specified register;
- in the case of a foreign company, on the basis of the statements made by the party to the transaction.

886. Advocates and the management of law offices are subject to the MLTFPA.

887. Some guidelines have been issued since the 3rd round evaluation. The Bar Association Board issued guidelines on 9 September 2008 on procedural rules to fulfil the duties of impeding and forestalling money laundering and financing terrorism. The Management Board of the Estonian Bar Association amended it with a resolution on 18 June 2013: "*Law Firm's Rules of Procedure for performance the obligation to prevent money laundering and terrorist financing*". In the cases

as determined in the MLTFPA the attorney or the management of the law firms is required to follow these rules of procedures.

888. Attorneys who enter into a contract with their clients and provide legal services under the scope of the MLTFPA and the Rules of Procedure are required to conduct CDD, and also to preserve identification data and documents. Copies of documents should be preserved for at least five years after the business relationship ends. If relevant the date and period of a transaction is registered. Lawyers are required to apply the risk-based approach. Three risk categories are defined: geographic, client risk and risk related to the task performed. Rules of Procedure provide guidelines when risk is regarded high and the necessary measures. Procedures are also determined for identification of legal persons, PEPs, beneficial owners.

Implementation

889. The evaluators were informed that based on the MLTFPA, every notary is responsible for training all employees of his or her office who are involved in client-facing activities on CDD requirements.

890. The *notaries* met on-site were fully versed in their CDD obligations. The awareness in this sector seems to be high and the effectiveness of implementation is sufficient. Notaries stated that they always meet the customer or the representative in person. They confirmed that they used the risk based approach according to the requirements of the MLTFPA and the Instructions. However, the identification of source of funds was not confirmed by all representatives.

891. The evaluation team was informed that in the e-notary system, the data of each party is recorded and is available for the FIU and other relevant authorities on a timely basis.

892. The meetings with *sworn advocates* and the representatives of the *Bar Association* indicated a satisfactory level of knowledge of the requirements of the MLTFPA and the effectiveness of implementation seems to be sufficient. The evaluators were informed that the customer and beneficial owner information is obtained and verified based on reliable sources, eg. publicly available State registers of Estonia, commercial register and in case of non-residents via Internet. However in view of the evaluators the procedures of verification of the information of the beneficial owners only from the mentioned registers do not seem to be sufficient as these not necessarily contain the required information on BO. In case of higher risk customers extra documentation is required to be submitted. The identification of source of funds was confirmed to be verified.

893. Advocates stated that they do not enter into a business relationship and do not provide legal assistance until they understand the structure, business and operations of the legal entity and they have the necessary information on the beneficial owner and the customers provide additional information on the purpose of the business relationship.

894. Advocates do not have lists to be used upon applying CDD, e.g. PEP list but they receive all necessary information from the Bar Association and the FIU.

895. The FIU confirmed that the lawyers who are supervised by the FIU also have internal procedures in place.

896. *Auditors* and *providers of accounting services* as well as *providers of accounting or tax advice services, and bankruptcy trustees* also fall within the scope of the MLTFPA.

897. All requirements of the MLTFPA shall be applied for the auditors, providers of accounting services as well as providers of accounting or tax advice services, there are not specifications determined. The FIU has issued advisory guidelines for auditors and providers of accounting services to explain legislation based on Art. 39(1) of the MLTFPA.

898. The evaluators were informed that the new Auditors Activities Act entered into force 8 March 2010. Remarkable changes concerning the supervisory regulation of auditors and implementation of new standards were introduced. Most important changes in new Auditors Activities Act: a public register has been set up that includes all properly recognized auditors and audit firms, all auditing activities are now based on international standards which have been translated and adopted on a national level, exams and qualifications system for auditors, based on international standards has been created, sworn auditors and auditor firms have been subjected to public oversight and to quality control by professional association.

Implementation

899. Auditors and accountants met on-site appeared to have adequate knowledge of AML/CFT requirements. The representatives showed awareness on the legal provisions of the MLTFPA and the guidelines of the FIU which they considered to be a useful in the everyday practice. They have taken part in several trainings organised by the FIU and the Estonian Board of Auditors. They confirmed that they have internal procedures in place and they did not mention any difficulties as regards the interpretation of the legal provisions of the MLTFPA and implementation of the requirements in their everyday practice. They apply CDD measures however the procedures based on risk based approach was not convincing.

900. To further increase the awareness of DNFBP sector, the FIU has provided several trainings. In 2009 training was provided to the Bar Association (100 attorneys participated). Additionally, the FIU provided six AML/CFT training sessions for notaries, auditors, accountants and other DNFBPs (in total cca 200 participants). In 2010 a training session was provided to accountant service providers (16 participants), and one to auditors (30 participants). In 2011 the FIU provided training for Bar Association (160 participants). The issues of the training covered all AML requirements in the MLTFPA, in 2010 mainly the changes and the interpretation of the provisions of the law. FIU focused on sector specific interpretation of the obligations, the application of CDD measures as well as on the notification.

*Trust and company service providers*

901. According to Art. 7 of the MLTFPA, a provider of trust and company services is a natural or legal person who in their economic or professional activities provides a third party with no less than one of following services:

> *"1) foundation of a company or another legal person;*
>
> *2) acting as a director 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 this position by another person;*
>
> *3) enabling use of the address of the seat or place of business, including granting the right to use the address as part of one's contact information or for receiving mail as well as providing companies or other legal persons, civil law partnerships or other similar contractual legal arrangements with services relating to the aforementioned;*
>
> *4) acting as a representative of a civil law partnership or another such contractual legal arrangement or appointing another person to the position;*
>
> *5) acting as a representative of a shareholder of a public limited company or arrangement of representation of a shareholder by another person, except in the event of companies whose securities have been listed in a regulated securities market and with respect to whom disclosure requirements complying with European Community legislation or equal international standards are applied."*

902. According to Art. 52(1)2), the providers of trust and company services are required to register themselves in the register of economic activities before commencing operations in the corresponding area of activity.

903. Although trust service providers are obligated persons under the MLTFPA, there are no such entities operating in Estonia. Trust as a legal arrangement is not recognized in the Estonian legal system. In accordance with Art. 7 and 26 of the General Part of the Civil Code Act (GPCCA), a natural person and a legal person have passive legal capacity (the capacity to have civil rights and perform civil obligations).

904. On the basis of information provided in the questionnaire, the term "*trusts"* in Estonian laws is a reference to fiduciary relationships and not to trusts as understood in Common Law system. Legal relationships resembling those of a trust may arise in Estonia in connection with a civil law partnership or another similar contractual legal entity regulated by the Law of Obligations Act. According to the meaning of the 3rd AML/CFT Directive, the issue of trusts and other similar legal entities must be dealt with in national law regardless of whether the national law of the specific Member State regulates trusts or not. Legal relationships resembling those of a trust may arise in Estonia in connection of a civil law partnership or another similar contractual legal entity.

905. According to the MLTFPA there are no further measures determined for trusts.

906. There is however a small category of entities providing company services. These total 70 in all and are subject to FIU supervision. None were met on-site. The FIU informed the evaluation team that it had conducted a number of onsite visits with the main purpose of raising awareness (see further under Recommendation 24). The FIU confirmed that these entities have internal rules of procedures and apply CDD measures and register CDD data. The evaluation team could not confirm this information.

907. According to the FIU, company service providers are not considered to pose a high ML/FT risk since they only service a limited number of domestic customers who need assistance in setting up a company. Most companies in Estonia are set up by the directors/respresentatives of the company themselves through a simple online procedure.Additionally, all company service providers are required to register in the register of economic activities before commencing operations in the corresponding area of activity.

*Applying Recommendations 8 (c. 12.2)*

908. The same requirements which apply to financial institutions also apply to DNFBPs. If relevant, rules of procedures should cover the procedures when new technologies are used or intended to be used. For an analysis of the provisions in Estonian law which implement Recommendation 8 see section xx.

909. The FIU has also issued a guidance (which was approved by the Governmental Committee and Advisory Committee) on CDD measures of non-face-to-face businesses. The guidance has been issued for explaining requirement provided for in clause 19(2)1) of the MLTFPA.

910. As regards the ML threats that may arise from new technologies and non-face-to-face businesses most of the representatives stated that they usually meet in person and they receive all necessary information from the FIU.

*Applying Recommendation 10 (c. 12.2)*

911. Provisions as regards record keeping apply to DNFBPs in the same way as they apply to financial institutions. The findings for credit and financial institutions also apply in this case (see above under R. 10).

Implementation

912. The evaluators were convinced by the explanations provided by DNFBPs met onsite, except for real estate agents, on the record-keeping measures that are implemented. Most of the representatives of DNFBPs confirmed that the information is registered and available on a timely basis for the FIU and other competent authorities. In case of lawyers the sensitive information as well as information of attorney-client privileged is discussed with the Bar Association before disclosing information to the competent authorities.

*Applying Recommendation 11(c. 12.2)*

913. With regard to criterion 12.2 and the application of Recommendation 11, the comments and observations made for credit and financial institutions under Recommendation 11 equally apply for DNFBPs as the relevant provisions of MLTFPA apply to both financial institutions and DNFBPs.

***Effectiveness and efficiency***

914. With the amendments in the MLTFPA, Estonia rectified several deficiencies identified in the 3rd round MER in relation to the CDD requirements. However, further legislative clarifications and improvements are still needed for full compliance with the standards. Furthermore, there remain some concerns regarding the effective implementation.

915. In Estonia the coverage of DNFBPs is complete and in line with international standards.

916. The FIU has issued guidelines to some specific sectors and on specific issues. All the guidelines are available on-line.

917. As the relevant provisions of the MLTFPA apply both to financial institutions and DNFBPs in the same way, except for some specifications, the comments and observation made for credit and financial institutions under Recommendation 5, 8, 10 apply for DNFBPs.

918. Overall the meetings with the private sector demonstrated a satisfactory level of awareness and good understanding of the CDD and record keeping obligations under the MLTFPA (apart from the above mentioned exemptions). Most of the representatives of the DNFBPs showed awareness of sector specific and currents risks and vulnerabilities of ML and TF. They have also internal procedures in place. However, based on the evaluators propose further awareness-raising on the risk based approach. The source of funds of the customer is not registered, not even in case of PEPs or high risk customers.

919. The notaries are fully versed in their obligations. The identification and verification of the client is complete, and compliant with the standard. Risk factors and processes are introduced in their internal procedure and practice. The awareness in this sector seems to be high and the effectiveness of implementation is sufficient.

920. Lawyers met onsite have a wide knowledge on AML/CFT and preservation requirements. Risk-based approach has been introduced in the everyday practise. The rules of procedure for law firms issued by the Estonian Bar Association are regarded to be very useful by the representatives met onsite. Evaluators are not aware of any guideline published by the FIU for those lawyers who are not supervised by the Estonian Bar Association, however, the FIU confirmed that they have proper rules of procedures in place.

921. The evaluators were informed that there are 121 companies holding an active registration for buying-in or wholesale of precious metals. The registration for retail-sales is of a wider nature: before commencing any retail-sales activities a retail-sales registration in the Registry of Economic Activities has to be made and if precious metals will (additionally or separately) be sold, a separate box on the registration form has to be ticked.

922. Auditors confirmed that they have internal procedures in place and they did not mention any difficulties as regards the interpretation of the legal provisions of the MLTFPA and implementation of the requirements in their everyday practice. They are aware of the AML/CFT requirements, apply CDD measures however the procedures based on risk based approach might be needed to be further developed.

923. The evaluators did not meet the representatives of company service providers. This sector is considered to be a less risky one by the authorities.

924. With regard to all DNFBPs the Estonian authorities should apply recommendations and comments made under Recommendations 5, 8 and 10 in relation to the financial institutions.

925. It is the view of the evaluators, that more awareness-raising activities are needed as regards the requirements of the MLTFPA for real estate agents and dealers in precious stones and metals. There is a need for a broad outreach to the sector of real estate agents and wholesalers of precious stones and metals. Sector specific guidelines or training (on verification of legal persons, beneficial ownership and risk based approach) would be needed by the FIU.

### 4.1.2 Recommendations and Comments

***Applying Recommendation 5***

926. The Estonian authorities should apply the recommendations made under Recommendations 5 in relation to financial institutions.

927. The Estonian authorities should also:

- strengthen the awareness and effective implementation of the risk based approach (extent of CDD requirements);
- strengthen the awareness and effective implementation of identification and verification of source of funds, at least in high risk cases and customers;
- strengthen the awareness and effective implementation of beneficial owner;
- strengthen effective implementation of the CDD requirements with regard to *real estate agents;*
- strengthen effective implementation of the CDD requirements with regard to *dealers in precious metals and dealers in precious stones (and high value dealers)*;

***Applying Recommendation 10***

928. The Estonian authorities should apply the recommendations made under Recommendations 10 in relation to financial institutions.

929. Estonian authorities should strengthen effective implementation of the record-keeping requirements with regard to real estate agents.

***Recommendation 11***

930. The Estonian authorities should apply the recommendations made under Recommendations 11 in relation to financial institutions.

931. In terms of effectiveness, DNFBPs who were interviewed during the onsite confirmed that in practice they do examine unusual transactions and that the findings of such examinations are recorded.

4.1.3 Compliance with Recommendation 12

| | Rating | Summary of factors relevant to s.4.1 underlying overall rating |
|---|---|---|
| **R.12** | **PC**[68] | ***Applying Recommendation 5***<br>• No clear requirement to determine whether the customer is acting on behalf of another person;<br>• No requirement to apply CDD requirements to existing customers;<br>**Effectiveness**<br>• Weakness in the implementation of the identification and verification of source of funds, especially in case of higher risk customers and PEPs;<br>• Some shortcomings in the implementation of risk-based approach (extent of CDD measures);<br>• Weakness in the implementation of CDD measures by real estate agents;<br>• Some deficiencies in the implementation of CDD measures of dealers in precious metals and dealers in precious stones.<br>***Applying Recommendation 10***<br>• No provision in law or regulation to ensure that the mandatory record-keeping period may be extended in specific cases upon request of competent authorities (as preventive measures);<br>**Effectiveness**<br>• Lack of effective implementation of the record-keeping requirements with regard to real estate agents.<br>***Applying Recommendation 11***<br>• The requirement to pay special attention to complex, unusual large transactions does not apply to "patterns of transactions" as required by the criterion;<br>• The requirement to pay special attention does not apply to transactions which have "no apparent or visible lawful purpose" as required by the criterion;<br>• No clear requirement to examine the nature, purpose or background when discovering a complex or unusual transaction during transaction monitoring;<br>• No clear obligation to keep records of findings that do not lead to |

[68] The review of Recommendation 12 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 6 and 9.

| | | |
|---|---|---|
| | | STR. |

## 4.2. Suspicious transaction reporting (R. 16)

(Applying R.13 to 15 and 21)

4.2.1 Description and analysis

***Recommendation 16 (rated PC in the 3rd round report)***

*Applying Recommendation 13*

*Requirement to Make STRs on ML/FT to FIU (c. 16.1; applying c. 13.1 & c.13.2 and SR. IV to DNFBPs)*

932. As a rule, all DNFBPs listed in Art. 3 MLTFPA are subjected to the same reporting duty as the credit institutions when acting in their professional capacity, performing economic activities or official acts (Art. 32(1) to (3) MLTFPA). Concretely this applies to casinos ("organisers of games of chance – art. 3(1)3), real estate agents (art. 3(1)4), dealers in precious metals or stones (art. 3(1)5 & 6.1), auditors and accountants (art. 3(1) 7&8), trust and company service providers (art. 3(2)9) and – in certain circumstances - legal professionals (art. 3(2)) (see also Rec 12 above)).

933. Thus the obligation relates to reporting suspicious activity, currency transactions exceeding 32,000 EUR and attempts in the circumstances of Art. 27(6) 1 to 3 MLTFPA. As is the case with financial entities, the disclosures have to be made "immediately" or at least within two working days, both for SARs and CTRs. The DNFBPs equally have the "right" to postpone the transaction or operation before notifying the FIU.

934. As with financial institutions the suspicious activity reporting duty relates to indications of (attempted) money laundering or terrorism financing. As stated above in the context of R13 the reference to terrorism financing falls short of the international standard imposing a reporting duty on funds suspected to be related or used for terrorism, terrorist acts or by terrorist organisations, beside the persons financing terrorism.

*Legal Privilege*

935. Professionals bound to a legal privilege, *i.e.* notaries and lawyers (attorneys) fall under an exceptional regime (Art.32(4) MLTFPA). They are under no obligation to report when they provide counsel on the client's legal position or represent their client in legal proceedings. The principle of legal professional privilege applies in all court proceedings to allow for effective protection of clients' interests.

936. The confidentiality of the relationship between an advocate and their client is however not absolute. According to the explanatory memorandum to the MLTFPA Art. 32(4), the legal professional privilege does not extend to cases where an attorney or notary public acts as a representative of the client in financial or real estate transactions. It also does not extend to the provision of a legal service in respect of managing or implementing a transaction involving the purchase or sale of real estate, financial management of assets, opening bank or securities accounts, acquisition of funds required for the foundation, operation or management of a company or foundation, management of a trust, company or other similar entity, or in carrying out an official act. The immunity obviously also does not apply if the legal professional is an accomplice to money laundering or terrorist financing activity, if legal advice is given for the purpose of money laundering or terrorist financing or if the layer or notary public knows that the client wants legal advice for the purpose of money laundering or terrorist financing.

*No Reporting Threshold for STRs (c. 16.1; applying c. 13.3 to DNFBPs)*

937. The reporting duty is not limited in terms of a minimum or maximum amount, and includes attempts. Reference is made to the comments under R.13 on this point.

*Making of ML/FT STRs regardless of Possible Involvement of Tax Matters (c. 16.1; applying c. 13.4 to DNFBPs)*

938. The presence of fiscal aspects is completely irrelevant and without impact on the reporting duty laid down in Art. 32 MLTFPA.

*Reporting through Self-Regulatory Organisations (c.16.2)*

939. All DNFBPs subject to the reporting duty must file their SARs or CTRs directly to the FIU, without passing through any SRO.

*Applying Recommendation 21*

940. With regard to criterion 16.3, the comments and observations made for credit and financial institutions under Recommendation 21 equally apply for DNFBPs as the relevant provisions of MLTFPA apply to both financial institutions and DNFBPs.

941. In addition, while the FSA issues circular letters to inform supervised entities of the content of FATF Public statements and advises the institutions to consider the risks arising from the deficiencies associated with each jurisdiction mentioned in the statements and apply according counter-measures, these circular letters are not sent to DNFBPs.

***Effectiveness and efficiency***

*Applying Recommendation 13*

The table below shows the number of SARs sent by the DNFBP sector:

**Table 25: SARs by category of DNFBP**

| | **2008** | | **2009** | | **2010** | | **2011** | | **2012** | | **2013** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | SAR | CTR | SAR | CTR | SAR | CTR | SAR | CTR | SAR | CTR | SAR | CTR |
| Traders | 23 | 131 | 5 | 118 | 2 | 128 | 28 | 168 | 20 | 169 | 4 | 43 |
| Real estate dealers | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| Gambling Organisers | 37 | 315 | 2 | 330 | 5 | 195 | 3 | 358 | 11 | 571 | 20 | 475 |
| Attorneys | 6 | 0 | 4 | 0 | 5 | 0 | 0 | 5 | 5 | 4 | 10 | 0 |
| Auditors/Accountants | 3 | 3 | 3 | 16 | 0 | 11 | 5 | 27 | 1 | 20 | 0 | 37 |
| Bailiffs | 1 | 0 | 0 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 2 |
| Notaries | 53 | 170 | 50 | 118 | 59 | 93 | 26 | 72 | 41 | 86 | 49 | 125 |
| Bankruptcy Trustees | 0 | 1 | 4 | 0 | 5 | 4 | 4 | 0 | 5 | 0 | 4 | 1 |
| **TOTAL** | **86** | **174** | **69** | **583** | **77** | **434** | **68** | **631** | **84** | **851** | **90** | **683** |

942. The latest figures show a notable rise in the number of CTRs sent in by the gambling industry and the traders, indicating an increased use of cash in these sectors. More importantly the reporting behaviour in terms of the number of SARs is variable, generally without raising significant concerns. There are however still some sectors clearly under-reporting, particularly and typically the real estate agents who conveniently pass the reporting duty to the notaries involved in the actual financial transactions, whilst ignoring that their own obligations already start with the establishment of the commercial relation. The low scale of reporting by bailiffs, bankruptcy trustees and attorneys, although less pronounced, also merits further attention. It is encouraging however that the Estonian attorneys seem to take their reporting obligation more seriously than in most countries.

*Applying Recommendation 21*

943. The same deficiencies in the implementation of Recommendation 21 in respect of financial institutions apply equally to DNFBPs in the context of Recommendation 16.

944. In terms of effectiveness, not all DNFBPs who were interviewed during the onsite demonstrated an awareness of any obligation to examine transactions from countries which do not or insufficiently apply FATF Recommendations. Similarly, not all entities kept records of examinations of such transactions.

### 4.2.2 Recommendations and comments

*Applying Recommendation 13*

945. The reporting duty for DNFBs is fully within the international standards. The boundaries of the legal privilege exception are clearly defined and no instances of abuse have been reported. Otherwise all comments relating on the implementation of Recommendation 13 are also relevant in the DBNFBP context. Particularly, the underperforming real estate sector requires closer attention and more awareness raising, if needed by applying exemplary and effective sanctions.

*Applying Recommendation 21*

946. The same deficiencies in the implementation of Recommendation 21 in respect of financial institutions apply equally to DNFBPs in the context of Recommendation 16.

947. In addition, the FIU should consider issuing specific guidance to DNFBPs in relation to this obligation.

### 4.2.3 Compliance with Recommendation 16

| | Rating | Summary of factors relevant to s.4.2 underlying overall rating |
|---|---|---|
| **R.16** | **PC**[69] | *Applying Recommendation 13*<br>• No requirement to report suspicions on funds linked or related to, or to be used for, terrorism, terrorist acts or by terrorist organisations or those who finance terrorism; |

[69] The review of Recommendation 16 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 14 and 15.

| | | |
|---|---|---|
| | | **Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness;<br>• Underreporting by certain DNFBPs.<br>*Applying Recommendation 21*<br>• Technical deficiency in relation to the application of the obligation to a customer or person from one of the stipulated countries;<br>• 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;<br>• No clear requirement to keep records of findings that do not lead to STR;<br>**Effectiveness**<br>• No awareness-raising by the authorities to DNFBPs on jurisdictions which do not or insufficiently apply FATF Recommendations;<br>• Weak awareness of this requirement by certain DNFBPs. |

## 4.3. Regulation, supervision and monitoring (R. 24-25)

**Summary of third round MER factors underlying ratings and recommendations**

948. The MER rated Recommendation 24 as Partially Compliant. Recommendation 25 was rated as Partially Compliant. These were based on the following factors:

- Lack of fit and proper tests for beneficial owners and managers of casinos;
- Not all trust and company service providers required to be registered;
- No supervision for legal professionals who are not members of the Bar Association;
- Lack of adequate mechanisms for supervision by the Chamber of Notaries and the Bar Association;
- Lack of sufficient supervisory staff in the FIU;
- Insufficient guidance to DNFBPs by the FIU, the Chamber of Notaries and the Bar Association.

4.3.1 Description and analysis

***Recommendation 24 (rated PC in the 3rd round report)***

*Regulation and Supervision of Casinos (c. 24.1, c.24.1.1, 24.1.2 & 24.1.3)*

949. According to the Gambling Act 2009 all gambling is licenced, regulated and supervised by the Tax and Customs Board. The FIU is responsible for AML/CFT regulation and supervision of casinos (Art. 47 of the MLTFPA).

950. The terms and conditions for acquiring a qualifying holding in a gambling company, including the grounds for prohibition are set out in Art. 11—15 of the Gambling Act.

951. These state that the Tax and Customs Board may prohibit the acquisition of a qualifying holding if (inter alia) the acquirer of the qualifying holding does not have impeccable business reputation or does not meet the requirements provided for in this Act.

952. Under Art. 16—19 of the Gambling Act, the managers of casinos (and other organisers of gambling, incl. betting, skill games and lotteries) are subject to fit and proper checks before a licence is issued.

953. Under Art. 17, applicants must provide "information and documents regarding the members of the management board and supervisory board of the applicant for an activity licence, including, for each person, the forename and surname, personal identification code or date of birth in the absence of a personal identification code, place of residence, a complete list of places of employment and positions and documents which prove the trustworthiness of the members of the management board and supervisory board of the applicant…" along with relevant information on shareholders and persons with qualifying holding.

954. Article 18 requires the Tax and Customs Board to consider (inter alia) "the trustworthiness and good reputation of the applicant" and "the work experience, business connections, education, trustworthiness and reputation of members of the management bodies of the applicant".

955. Article 19 provides that a licence shall be refused if the Tax and Customs Board has become aware of information indicating that the applicant for the activity licence is not a trustworthy person.

956. The Tax and Customs Board has 4 staff responsible for gambling licencing and supervision. Fit and proper checks undertaken by staff always include criminal records checks, for both domestic and overseas individuals involved in owning or managing an applicant.

957. Decisions on fitness and propriety are made on a case by case basis, with a conviction connected to gambling, tax, money laundering or any other financial offences being sufficient to deny an application.

958. The FIU is the authority responsible for ensuring that gambling operators comply with the MLTFPA, and supervises casinos for that purpose. The supervisory powers of the FIU are set out in MLTFPA – Art. 48. A detailed description of the FIU's regulatory and supervisory powers are set out under Section 3.7 of the report, which are applicable to both financial institutions and certain DNFBPs. In addition, Art. 20 of the Gambling Act states that repeated violations of AML/CFT procedures is sufficient grounds to revoke the activity licence of the gambling company.

*Monitoring and Enforcement Systems for Other DNFBPS-s (c. 24.2 & 24.2.1)*

959. The MLTFPA states that the FIU is responsible for supervising all categories of DNFBP (with several exceptions as noted below) in relation to compliance with AMLCFT requirements.

960. This includes Trust and company service providers, defined in Art. 7 of the MLTFPA to include any natural or legal person who in their economic or professional activities provides a third party with trust and company services.

961. Article 47 of the MLTFPA states that the Estonia Bar Association is responsible for supervising its members for compliance with MLTFPA. Similarly, the Ministry of Justice is responsible for the supervision of notaries public.

962. The FIU, the Bar Association and the Ministry of Justice (acting through its delegate, the Chamber of Notaries) may exercise all the powers set on in Art. 48 MLTFPA.

963. Article 48 of the MLTFPA include the power to carry out on-site inspections and obtain documents, information and oral or written explanations:

> *"(1) The supervisory authority has the right to inspect the seat or the place of business of obligated persons. The supervisory authority has the right to enter a building and room that is in the possession of an obligated person in the presence of a representative of the inspected person.*
>
> *(2) In the course of an on-site inspection the supervisory authority has the right to:*
>
> *1) without limitations inspect the required documents and data media, make extracts, transcripts and copies thereof, receive explanations regarding them from the obligated person, and monitor the work processes;*
>
> *2) receive oral and written explanations from the obligated person being inspected, members of its directing body or employees.*
>
> *(3) The supervisory authority has the right to, without carrying out any on-site inspection, demand by a precept that the obligated person submit information required for inspection."*

964. There is no legislative provision or guidance defining "information required for inspection" in Art. 48(3), but the FIU confirmed that this is interpreted to include any information concerning the obligated person's compliance with the MLTFPA. Questionnaires used by the FIU to conduct off site supervision have required obligated persons to provide both descriptions and copies of internal policies procedures and controls.

965. As discussed in detail in Section 3.7, these provisions appear to contain all elements required by the criterion and are being implemented by the FIU in a manner consistent with that interpretation.

966. However, the Bar Association and the Chamber of Notaries do not exercise supervisory powers pursuant to the MLTFPA, but rather exercise powers in Bar Association Act and the Notaries Act, which provide general powers of supervision over their members.

967. Article 3 of the Bar Association Act states that:

> *"The Bar Association is competent to:1) …2) exercise supervision over the processional activities of the members of the Bar Association and their compliance with the requirements for professional ethics; 3) …"*

968. While these provisions do not explicitly refer to onsite inspections or the collection of documents and information, the Bar Association does, in fact, exercise supervision by way of on-site inspections.

969. Article 5 of the Notaries Act states that:

> *"1) The Ministry of Justice shall supervise the professional activities of notaries. The Ministry of Justice may involve the Chamber of Notaries in the supervision activities.*
>
> *(2) The Ministry of Justice may delegate supervision over compliance with the requirements of the Money Laundering and Terrorist Financing Prevention Act and legislation established on the basis thereof and supervision over other individual matters to the Chamber of Notaries. In the delegated area of supervision, the Ministry of Justice may give instructions for the exercise of supervision and amend resolutions adopted by the Chamber of Notaries with respect to such areas.*
>
> *(3)…*

*(4) Supervision means periodical inspection over professional activities of notaries. Additional inspection is allowed only in justified cases where there is information referring to the need of inspection. In the case of a new notary, the first inspection shall be conducted within the notary's second year of office.*

*(5) A notary is required to present the books concerning his or her professional activities and other materials which are necessary for the supervision activities."*

970. Similarly, administrative sanctions may be applied against notaries public and members of the Bar Association pursuant to the Bar Association Act and the Notaries Act.

971. Article 19 of the Bar Association Act provides for the imposition of penalties for "violation of legislation which provides for the activities of advocates", the penalties being reprimand, fine of up to 2 months earnings, suspension, or disbarment.

972. The Government of Estonia states that the Minister of Justice has the authority to impose a disciplinary penalty on a notary; namely reprimand, fine or removal from office. No statutory references have been provided to the assessors.

***Recommendation 25 (rated PC in the 3rd round report)***

**Guidance for DNFBPs other than feedback on STRs (c. 25.1)**

973. Article 44 of the Notaries Act provides that the Chamber of Notaries may prepare guidelines for the harmonization of the practice of notaries related to office.

974. The Chamber of Notaries issued a guideline on 1 November 2008, which was subsequently updated on 26 March 2010. This contains rules of procedure for the due diligence measures required by MLTFPA, as well the rules of internal procedure for checking the implementation of the measures. They do not contain guidance on the ML/TF methods and techniques.

975. Similarly, the Bar Association Board issued guidelines on 9 September 2008, which was subsequently updated on 18 June 2013. This contains procedural rules to fulfil the AML/CFT obligations, but does not contain guidance on the ML/TF methods and techniques.

976. The FIU has issued the following guidelines in order to assist the entities it supervises:

- auditors and providers of accounting services;
- traders;
- pawn houses;
- casinos;
- notaries public (in cooperation with Chamber of Notaries).

**Feedback (applying c. 25.2)**

977. Since 2005 the Estonian FIU has published an annual report, which contains, *inter alia*, sanitized cases, typologies and existing and emerging ML trends.

978. In addition the FIU is empowered by Art. 39 of the MLTFPA to issue advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing. FIU has issued guidelines to specific subsectors which include guidance (general feedback) on indicators of money laundering and the financing of terrorism

979. In relation to case by case feedback, the FIU provides an annual feedback notice to each reporting entity, where an SAR has been forwarded to a law enforcement authority or a Prosecutor's Office for further investigation. The FIU also updates the reporting entity on the results of the investigation (e.g. case is closed or completed) and possible convictions/acquittals.

***Adequacy of resources supervisory authorities for DNFBPs (R. 30)***

980. The Tax and Customs Board is a public body tasked with (inter alia), ensuring the receipt of state budget revenue from state taxes and customs duties. It is also responsible for the issue of operating permits for gambling and for organisers of lotteries, for which it has sufficient financial, human and technical resources.

981. The FIU is an independent structural unit of the Police and Border Guard Board, pursuant to Art. 36(1) of the MLTFPA. The FIU is funded as any other unit within Central Criminal Police and Art. 36(3) of the MLTFPA requires the Police and Border Guard Board to provide the FIU with sufficient funds for performance of the functions provided by law.

982. Analysis of the training and integrity of FIU staff is included under Recommendation 23.

983. The number of obligated persons is large and requires the allocation of substantial human resources to ensure effective supervision by the FIU. The FIU has its own permanent staff (currently 18), a dedicated database and access to all available information which is necessary to perform their duties. At the time of the onsite, the FIU had 4 staff in its Supervision Division responsible for supervising obliged persons' compliance with the MLTFPA (both financial institutions and DNFBPs). These staff also have non-supervisory responsibilities.

984. In the 3rd round MER, at paragraph 760, assessors recommended that additional staff should be provided by the FIU to ensure adequate and effective supervision of all obligated entities subject to its supervision. It does not appear that such additional supervisory staff have been provided.

985. The Chamber of Notaries is financed through membership fees paid by notaries and its activities are regulated by the Notaries Act. One of the principal tasks of the Chamber of Notaries is to participate in supervising the professional activities of notaries. The executive and organising body is the Board of the Chamber of Notaries, comprising seven members elected by Chamber of Notaries for a period of three years. The employees of the Chamber of Notaries are required by the Notaries Act to have necessary education, sufficient experience and professional qualifications to perform their duties and an impeccable reputation.

986. It has 1 member of staff responsible for AML supervision, who (accompanied by members of the Ministry of Finance) conducts onsite inspections of approximately 12% of its members per year.

987. The Estonian authorities have stated that the staff of the Chamber of Notaries participate regularly in relevant training, seminars and courses.

988. The Bar Association is a self-governing professional association, funded through membership fees paid by its members. The activities of the Bar Association are regulated by Bar Association Act, which stipulates, amongst other things, that it shall operate pursuant to the law and good morals. The employees of the Bar Association are required by the Bar Association Act to have necessary education, sufficient experience and professional qualifications to perform their duties and an impeccable reputation.

989. The Bar Association has 4 members of staff responsible for AML matters, 2 of whom conduct onsite inspections of approximately 10% of its members per year.

990. The Estonian authorities have stated that the staff of the bar Association participate regularly in relevant training, seminars and courses.

**Effectiveness and efficiency (R. 24-25)**

991. Since the last MER, the Estonian Authorities have introduced sufficient legal and regulatory arrangements to prevent criminals from owning or operating casinos. Market entry and fit and

proper requirements are effectively implemented by the Tax and Customs board who have 4 specialist staff responsible for gambling licencing and supervision and who undertake adequate fit and proper checks including domestic and overseas criminal records checks on all individuals involved in owning or managing a casino.

992. The FIU uses a risk model to determine its supervisory priorities and to plan on-site and off-site actions. Onsite supervision is generally undertaken for 2 purposes: awareness raising visits to members of a subsector (generally repeated every 3 to 5 years) and targeted on-sites to individual entities selected due to intelligence collected, complaints or SAR reporting behaviour. Supervisory resources are thus mainly focussed on individual entities that are highlighted by receipt of adverse information, with less consideration of the inherent ML/TF risks of subsectors.

993. On-site inspections are carried out by at least 2 staff members. On-site inspections are usually conducted on notice, although not when there is a risk that advance notice may inhibit the effectiveness of the on-site inspection.

994. The obliged entity is normally required to deliver information in advance of the inspection. This means that some analysis is conducted by FIU staff prior to the inspection itself.

995. There is no internal methodology or "check-list" used by staff in planning or undertaking an onsite inspection. FIU staff stated that the contents of an onsite inspection are always consistent and include all aspects of AML compliance obligations, including sample testing.

996. Following an onsite inspection, an inspection report is prepared by staff, summarising the finding of the inspection. This is submitted to the Head of the FIU, who makes the decision on whether to apply a sanction. There are no specific decision making criteria in this regard. FIU staff stated that, in the case of an "awareness raising" inspection, the policy was to be more lenient in relation to compliance failures. This was because the inspection is often the entity's first contact with the FIU and the entity was often unaware of its obligations.

997. FIU staff suggested that off-site supervision was "not really used any more". Historically, the FIU had used questionnaires and surveys primarily to identify which entities were undertaking activities that are subject to AMLCFT obligations. Use of this tool reduced off from 2010, once these entities were identified.

998. Statistics on supervisory activities and sanctions levied by the FIU have been provided by the authorities as follows:

**Table 26: DNFBP supervisory actions by FIU:**

| | 2013 | | 2012 | | 2011 | | 2010 | | 2009 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Number of inspected enterprises | Number of commenced misdemeanour proceedings | Number of inspected enterprises | Number of commenced misdemeanour proceedings | Number of inspected enterprises | Number of commenced misdemeanour proceedings | Number of inspected enterprises | Number of commenced misdemeanour proceedings | Number of inspected enterprises | Number of commenced misdemeanour proceedings |
| Casinos | 2 | | 6 | - | 4 | - | 1 | - | 28 | - |
| Pawn shops | 25 | 6 | 15 | 4 | 3 | 3 | 2 | - | 82 | 29 |
| Traders | 2 | 1 | 4 | 2 | 4 | - | 1 | - | 11 | 3 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Real estate companies | 1 | | - | - | - | - | 4 | - | 4 | - |
| Legal service providers | 1 | | - | - | 32 | - | 102 | - | 227 | - |
| Other companies | 22 | 4 | 7 | - | 2 | - | 12 | - | 1 | - |
| TOTAL | 53 | 11 | 39 | 9 | 56 | 10 | 147 | 13 | 435 | 54 |

999. It is not clear that staffing of the FIU in relation to AMLCFT supervision is adequate (4 staff, not full time on supervision matters). On-site supervision varies between sectors and is not clearly based upon the risks of that sector. This means that the frequency of inspections varies between the different subsectors, with some receiving little supervisory attention during the period covered by this report.

1000. A range of potential sanctions are available to the FIU (discussed under Recommendation 17), but in practice only misdemeanour proceedings are used, which decreases the effectiveness of the sanctioning powers.

1001. The Chamber of Notaries selects individuals for supervision inspection by a mixture of a rolling basis (with each individual visited every 5 to 8 years) and targeting by reference to complaints about non-AML/CFT related conduct. On site supervision consists of a visit of average 1 day, which covers compliance with all legal obligations (including AML). Off-site supervision is not undertaken.

1002. In the past three years supervision over notaries was conducted on 41 occasions. No disciplinary action has been taken related to compliance with MLTFPA.

1003. The Bar Association supervises its members by a mixture of random selection and members targeted on the basis of complaints about non-AML/CFT related conduct. On site supervision consists of a visit of average 2 hours, which covers compliance with all legal obligations (including AML). Off-site supervision is not undertaken.

1004. In past three years the Bar Association has undertaken 36 onsite supervision inspections. In 1 case a precept was issued because the individual did not have internal controls.

1005. The Bar Association and Chamber of Notaries have sufficient powers to conduct both on-site and off-site supervision of its members. Onsite supervision is not sufficiently comprehensive, nor applied on the basis of ML/TF risk. A range of sanctions are available, but no sanctions for AML failures have been imposed in the period covered by this report.

1006. Obligated persons interviewed during the onsite visit did, however, demonstrate sufficient awareness of AML/CFT obligations.

4.3.2 Recommendations and comments

**Recommendation 24**

1007. The Estonian authorities should review the risk model used by the FIU to ensure that appropriate resources are applied to all subsectors, as well as to those individual entities that present higher risk of money laundering or terrorist financing.

1008. The Estonian authorities should also review the staffing levels at the FIU to ensure that sufficient supervisory staff are in place to effectively cover the full range of entities supervised for compliance with AML/CFT obligations.

1009. The Bar Association and Chamber of Notaries should review the way they formulate their supervisory programmes, to ensure that resources are applied to those institutions or members that demonstrate the higher risk of money laundering or terrorist financing. They should also review the content of the supervisory interactions, to ensure that compliance with AML/CFT obligations is given sufficient attention during the onsite inspections.

1010. The Estonian authorities should review the sanctions available to the various supervisors under the MLTFPA, the Bar Association Act and the Notaries Act in order to ensure consistent application of disciplinary measure across all sectors.

1011. The FIU should also consider use of a wider range of sanctions, including public sanctions, financial penalties and sanctions against individuals where appropriate.

### 4.3.3 Compliance with Recommendations 24 and 25 (Criteria 25.1, DNFBPS)

| | Rating | Summary of factors relevant to s.4.3 underlying overall rating |
|---|---|---|
| **R.24** | **PC** | • Sanctions available for legal persons that are financial institutions do not extend to directors and senior management;<br>**Effectiveness**<br>• Insufficient supervisory resources at the FIU;<br>• In practice only misdemeanour proceedings are used by FIU;<br>• Low level of on-site visits for certain DNFBPs under FIU supervision;<br>• Insufficient supervision undertaken by the Bar Association and Chamber of Notaries;<br>• No sanctions imposed by either the Bar Association or Chamber of Notaries. |
| **R.25** | **C** | |

# 5. LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS

## 5.1. Legal persons – Access to beneficial ownership and control information (R.33)

**Summary of third round MER factors underlying ratings and recommendations**

1012. The MER rated Recommendation 33 as Largely Compliant. The following recommendations were made:

- Estonia should introduce control over the implementation of the obligation to submit updated information on ownership and control to the commercial register;
- Estonia should introduce supervision of the obligation of limited liability companies to maintain share and shareholder registers;
- Estonia should ensure that the legal framework ensures adequate, accurate and timely information on the beneficial ownership and control of legal persons.

***Recommendation 33***

5.1.1 Description and analysis

*Transparency of beneficial ownership and control and access to information (criteria 33.1 and 33.2)*

1013. The types of companies that can be formed in Estonia and the process for doing so are described in section 1 of this report.

1014. The relevant legislative provisions are set out in detail in section 5.1 of the 3rd round MER, which have not changed and therefore remain valid for the purpose of this assessment. Paragraphs 767 to 799 set out the assessors' analysis, which concludes that "All private and public limited companies must establish and maintain an updated register of shareholders, including their names and addresses. Share acquisitions and other changes to shareholdings must be entered in the company's share register and the shareholder register without delay. The register of shareholders or members is publicly available".

1015. However, assessors then went on to note that *"while all limited liability companies must keep share and shareholder registers, their compliance with this obligation is not supervised by any authority. There is limited cross-checking and examination of information submitted for these registers and limited procedures for updating of information once entered in a register"*.

1016. Assessors also noted that "there is no obligation for verification of documents or any kind of on-going supervision whether the data in the registers is still valid and accurate. Thus there are no sufficient measures to ensure updating of information on ownership and control of legal persons."

1017. Further, assessors noted that, while obligated entities must establish the beneficial ownership of their clients, *"information about beneficial ownership and control is not included in any registers. It is recommended that Estonia considers implementing a programme of monitoring or supervision of the full range of obligations of legal person to hold and submit updated information for the commercial registers. Furthermore, it is recommended that Estonia reviews its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership and control of legal persons"*.

1018. These identified deficiencies and suggested actions were not addressed in either of the 3rd round progress reports submitted by Estonia.

1019. No information regarding either the supervision of legal persons' compliance with registry obligations or any information in relation to the inclusion of beneficial ownership information in the commercial registries was provided by the authorities to the evaluation team.

1020. During the onsite visit, Estonian authorities confirmed that no checks are made on the accuracy and validity of information submitted to the various registers, nor is there any supervision of entities' compliance with obligations to keep information on the registers up to date and notify the registrar any changes. Authorities rely on the public nature of the registers to identify inaccuracies, false submissions or out of date information. Checks by the authorities are limited to checking whether information in annual returns (including information on beneficial ownership) corresponds to information previously submitted.

1021. According to Art. 61 of the Commercial Code, if the registrar has information concerning the incorrectness of an entry or that an entry is missing, the registrar may make the appropriate inquiries and, if necessary, may make or correct the entry. The registrar made 711 such enquiries in 2012 and 666 in 2013. In addition, if incorrect information is submitted to the commercial register, the persons who signed the petition is liable for any damage wrongfully caused.

1022. It is therefore unclear how information on beneficial ownership is maintained in Estonia where the shareholders/founders of a legal person established in Estonia are not natural persons and the shares are either held by another legal person or a nominee (in or outside Estonia). It is to be noted also that under the analysis of Recommendation 5 concerns are raised by the evaluation team regarding financial institutions' measures to determine who the beneficial owner is, especially in high risk situations. For instance, it was noted that statements obtained from customers indicating the identity of the beneficial owner are not signed by the beneficial owner himself. Additionally, as noted under the *Effectiveness* section of Recommendation 5, it is stated that knowledge and awareness of beneficial ownership requirements by certain financial institutions (especially payment services providers and currency exchange offices) was not adequate. In most cases, the identification and verification of beneficial owners of legal persons established in Estonia appeared to rely heavily on information provided by the client and information obtained from the Commercial Register, which does not maintain a register of beneficial ownership.

1023. As a result of these factors the evaluation team is of the view that it is doubtful whether competent authorities are in a position to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons.

*Prevention of misuse of bearer shares (c. 33.3)*

1024. Legal persons are not permitted to issue bearer shares in Estonia as Art. 228 of the Commercial Code requires all shares to be registered

*Additional element - Access to information on beneficial owners of legal persons by financial institutions (c. 33.4)*

1025. All information held on the registers is available to the public and readily accessible by financial institutions. This means that, if registered shareholders is also the beneficial owner, this information is publicly available. Where the beneficial owner is not a registered shareholder, no information is accessible.

**Effectiveness and efficiency (R. 33)**

1026. Estonia has a number of registries containing information about ownership and control of legal entities and has spent considerable resource introducing a comprehensive electronic system to provide access to market participants and the public.

1027. Company registration is available via an on-line portal, which allows the submission of electronic documents to the Department of Courts. This allows for the registration of private limited companies, sole traders and limited partnerships as well as the updating of information and the submission of annual reports. Security is maintained by way of ID card logging and digital signatures, which have the same legal effect as a notarised document.

1028. The Central Commercial Register is an online service which includes digital data from the commercial register, the register of NPOs and foundations and the commercial pledge register. Information is available both in Estonian and English and is accessible to the public via the internet. A free simple inquiry will reveal a business or association's name, registry code, status, share capital and address. A more detailed inquiry can also access more detailed information such as annual accounts and articles of association.

1029. The Visualized Business Register allows queries regarding persons related to companies and displays the results as a structure chart or diagram which gives an overview of the connections between legal persons and natural persons registered in the business register. The central database includes information from the commercial register, the register of NPOs and foundations and the commercial pledge register and can also access and display information from the Land Register and the European Business Register.

1030. Market participants that interviewed during the onsite confirmed the value of this resource in practice.

1031. Obligations to submit and update shareholder information to the register are clear and there are sanctions for non-compliance. For example according to PC and the Estonian Central Register of Securities Act all shares of public limited companies registered in Estonia should in registered and distributed through the Central Register of Securities. Other shares, subscription rights, units, holdings, issued debt obligations and other similar rights and obligations **may be entered** in the register unless otherwise provided by law. The shares of a company may be entered in the register only in the full amount of the share capital. Further, if the shares of the limited partnership are not registered in the ECRS a transaction constituting a share transfer must be notarised and lodged with the commercial register within two days**.**

1032. However, no checks are made on the accuracy and validity of information submitted to the register, which raises doubts as to the accuracy of the information on the register.

1033. While the registrar has taken action to correct inaccurate or missing information, including removal from the register, there is no active supervision of entities' compliance with obligations to keep information to up to date and notify any changes.

5.1.2 Recommendations and comments

1034. As suggested in the 3rd round mutual evaluation report and in the absence of any information or examples that indicate effective oversight of compliance with the obligations, the Government of Estonia should consider implementing a programme of monitoring or supervision of the full range of obligations on legal persons to hold and submit updated information to the commercial registers.

1035. In the absence of such supervision, it is difficult to demonstrate that ownership and control information is kept up to date and that adequate transparency is maintained.

1036. Also as suggested in the 3rd round mutual evaluation report, the Government of Estonia should consider reviewing its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership and control of legal persons.

1037. In the absence of such measures, adequate, accurate and timely information on the beneficial ownership of legal persons is not maintained and cannot be obtained or accessed in a timely fashion by competent authorities.

5.1.3 Compliance with Recommendation 33

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.33** | **PC** | • There is limited control over the obligations of legal persons to submit updated information on ownership and control to the register;<br>• Maintenance of share registers and shareholder registers by limited companies is not supervised;<br>• The legal framework does not ensure that information held in the Commercial Register is adequate, accurate and timely;<br>• It is doubtful whether competent authorities are in a position to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons. |

## 5.2. Non-profit organisations (SR.VIII)

5.2.1 Description and analysis

***Special Recommendation VIII (rated PC in the 3rd round report)***

1038. Special Recommendation VIII was rated PC in the 3rd round based on the following conclusions:

- No review of the adequacy of relevant laws and regulations to prevent the abuse of NPOs for financing of terrorism had been undertaken;
- Authorities had not conducted outreach or provided guidance on terrorist financing to the NPO sector;
- There was no supervision or monitoring of the NPO sector as envisaged by the Interpretative Note to SR VIII;
- There were no particular mechanisms in place for a prompt sharing of information among all relevant competent authorities when there was suspicion that a particular NPO was being exploited for terrorist financing purposes;
- No special points of contact or distinguished procedures to respond to international requests for information regarding particular NPOs.

*Legal framework*

1039. The Non-Profit Associations Act (NPAA) defines a non-profit association (NPO) as a voluntary association of persons the objective or main activity of which shall not be the earning of income from economic activity. The income of a non-profit association may be used only to achieve the objectives specified in its articles of association. A non-profit association shall not distribute profits among its members. A non-profit association is a legal person in private law. The passive legal capacity of a non-profit association commences as of entry of the non-profit association in the non-profit associations and foundations register (hereinafter *register*) and terminates as of deletion of the non-profit association from the register.

1040. Amendments to the NPAA were carried out in 2008 (which entered into force on 10 July 2008) to ensure that information in the register on NPOs is more reliable and transparent. As a result of such transparency, the authorities would also be in a better position to supervise the

economic activities of non-profit associations. The amendments also introduced the requirement on the management board of NPOs to prepare and submit annual accounts and activity reports at the end of each financial year. According to Art. $36^1$ of the NPAA the annual report is to be presented in electronic format to the court registrar within six months after the end of the financial year. The annual report is required to provide detailed information on the economic activities of the NPO. These reports and all other information on a NPO are open to public examination at the registry. Persons may obtain copies of registry cards and documents in the public files of non-profit associations.

1041. Amendments to the MLTFPA, which entered into force on 18 May 2012, brought NPOs under the scope of the Act whenever a cash payment of more than 15,000 EUR or an equal amount in another currency is made to a non-profit association or a foundation, regardless of whether the payment is performed in a lump sum or in several related payments. These amendments were prepared on the basis of an assessment of the sector carried by the FIU.

1042. The qualifying NPOs are therefore required to apply customer due diligence measures, maintain relevant records and report any suspicion of money laundering or terrorist financing to the FIU. This legislative measure could represent a good tool for further enhancing monitoring and supervision of a number of NPOs that might take part in such transactions, although it will not cover those NPOs which account for: (i) a significant portion of the financial resources under control of the sector; and (ii) a substantial share of the sector‘s international activities as required by the criterion c.VIII.3.

*Review of adequacy of laws and regulations (c.VIII.1)*

1043. The Estonian FIU conducted an assessment of the NPO sector based on the SARs received relating to the sector. The results of the assessment are described in the Explanatory Memorandum to 2012 amendments to the MLTFPA. In the period between 2008 and 2009 the FIU received 183 notifications concerning non-profit organisations (hereinafter NPO). Sixty threshold-based notifications were sent by one NPO, which qualified as a payment institution and was therefore required to report cash transactions. There were also serious suspicions of money laundering in several other cases which required in-depth analysis. As a result of the analysis, NPOs were included as reporting entities subject to FIU supervision according to the relevant provisions of MLTFPA.

1044. The assessment of the FIU also indicated that the risks of money laundering and terrorist financing for both external and internal security have increased in association with NPOs in 2012 and 2013. Although no court rulings had yet been made in the most serious cases, the FIU anticipated that the sector could give rise to significant risks in the future.

1045. As a result of this assessment, a number of amendments were carried out to the NPAA and the MLTFPA (see previous section ‘Legal Framework’). However, the assessment was conducted only on the basis of FIU information (SARs received) and the authorities did not explore and use all available sources of information of other state bodies for the purpose of identifying the features and types of non-profit organisations that are at risk of being misused for terrorist financing by virtue of their activities or characteristics. This should be taken into consideration while conducting periodic reassessments by reviewing new information on the sector‘s potential vulnerabilities to terrorist activities.

*Outreach to the NPO Sector to protect it from Terrorist Financing Abuse (c.VIII.2)*

1046. In order to provide outreach to the NPO Sector, the authorities invited a representative of the Network of Estonian Non-profit Organisations (NENO) to the Advisory Committee on Prevention of Money Laundering and Terrorist Financing (see Recommendation 31). NENO is the single and largest Estonian organization uniting public benefit non-profit organizations. NENO provides different advisory services and solutions to its member organisations via the portal

http://www.ngo.ee/en which has proven to be a good tool for information exchange to the NPO sector as the information network involves currently approximately 4,000 organisations. On the portal of NENO a webpage has been dedicated to AML/CFT issues.

1047. The evaluators welcome the authorities' initiative to include a representative from NENO in the Advisory Committee on Prevention of Money Laundering and Terrorist Financing. However, it should be noted that NENO involves approximately 4,000 NPOs, yet the number of registered NPOs in Estonia is much larger (29, 312 registered associations, 799 registered foundations and 580 registered churches and religious communities). Therefore, a small percentage of NPOs is subject to any outreach or awareness-raising activities.

*Supervision or monitoring of NPO-s that account for significant share of the sector's resources or international activities (c.VIII.3)*

1048. The authorities indicated that supervision of NPOs mainly consists in the review by the court register of the annual reports submitted by NPOs on an annual basis. Where a non-profit association fails to submit the requisite annual report in time, the court register is empowered to issue a warning to such association and require it to submit the annual report within a specified term which shall be at least six months. If, within six months the non-profit association fails to submit the annual report to the registrar, fails to provide a reasoned justification and the creditors of the association have not requested the liquidation of the association, the registrar may strike the association off the register. The court register only supervises the submission of the annual report and makes the report publicly available. The registrar (as the submission of annual reports is electronic, the information system) verifies whether the annual report contains all the needed parts and data required by law. The portal verifies the report automatically. The registrar has no competence to evaluate whether the data provided by the annual report is correct. While these measures are welcomed by the evaluation team, it appears that the court register is not conducting effective supervision or monitoring of those NPOs which account for: (i) a significant portion of the financial resources under control of the sector; and (ii) a substantial share of the sector's international activities as required by the criterion c.VIII.3.

1049. As indicated above, on the basis of an assessment produced by the FIU, the non-profit sector was brought within the scope of the MLTFPA whenever a cash payment of no less than 15,000 EUR or an equal amount in another currency is made to a non-profit association or a foundation, regardless of whether the payment is performed in a lump sum or in several related payments. Supervision of NPOs for AML/CFT purposes is exercised by the FIU. However, to-date, no supervision has been carried out since often the FIU is not in a position to determine those instances where the NPO receives cash payments above 15,000 EUR or equivalent sum. It was indicated that one NPO was included in the supervisory activity plan of the FIU for 2014. Activities conducted so far concerning the monitoring and supervision of NPOs do not appear to be sufficient.

*Information maintained by NPO-s and availability to the public thereof (c.VIII.3.1)*

1050. As indicated above, NPOs are required to submit annual accounts and activity reports at the end of each financial year to the court register. The annual report is required to provide detailed information on the economic activities of the NPO. These reports and all other information on a NPO are open to public examination at the registry. Persons may obtain copies of registry cards and documents in the public files of NPOs. Further information on the registration of NPOs and the public availability of information on the identity of persons who own, control or direct the activities of a NPO may be found in the Third Round MER which remains valid in this respect.

*Measures in place to sanction violations of oversight rules by NPO-s (c.VIII.3.2)*

1051. Article $36^1$ of the NPAA (Failure to submit annual report) prescribes that if a non-profit association fails to submit the requisite annual report to the registrar within six months after the

expiry of the term specified by law, the registrar shall issue a warning on deletion from the register to such person and obligate the person to submit the annual report within a specified term which shall be at least six months. Furthermore, every member of the management board may be punished separately by a fine for submission of incorrect information or failure to submit the prescribed information to the registration department of the court. Imposition of the fine may be repeated until the corresponding deficiency has been eliminated. The imposition of the fine should not preclude parallel civil, administrative, or criminal proceedings with respect to NPOs or persons acting on their behalf. Intentional submission of false information to the Register may be punished pursuant to criminal procedure by a fine or imprisonment for up to 2 years (PC Art. 281).

*Licensing or Registration of NPO-s and availability of this information (c.VIII.3.3)*

1052. NPOs are established as legal persons (either as associations or foundations) and are registered with County courts in the Non-profit Associations and Foundations Register. The information provided in the 3rd round MER on the applicable procedure remains valid.

*Maintenance of records by NPO-s, and availability to appropriate authorities (c.VIII.3.4)*

1053. Essential criterion VIII.3.4 requires NPOs to maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation.

1054. Authorities indicated that NPOs are required to maintain accounting records as all other legal persons in private law and their activities are subject to supervision by auditors (Art. 34, 35, 36, $36^1$ NPAA and Art. 33, 34, $34^1$, 35 Foundations Act). According to Art. 12 of the Accounting Act, an accounting entity shall preserve accounting source documents for seven years as of the end of the financial year during which the source document was recorded in the accounts. The management board organises the accounting of the NPO pursuant to the Accounting Act. After the end of a financial year, the management board shall prepare the annual accounts and activity report.

*Measures to ensure effective investigation and gathering of information (c.VIII.4)*

1055. As indicated above, NPOs are required to submit detailed information on their activities to the court registrar, which information is publicly available.

*Domestic co-operation, coordination and information sharing on NPO-s (c.VIII.4.1); Access to information on administration and management of NPO-s during investigations (c.VIII.4.2); Sharing of information, preventative actions and investigative expertise and capability, with respect to NPO-s suspected of being exploited for terrorist financing purposes (c.VIII.4.3)*

1056. Evaluators note that according to MLTFPA Art. 45 the Financial Intelligence Unit and the Internal Security Service cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information. The Director General of the Internal Security Service has appointed a contact person who has an equal right to an official of the Financial Intelligence Unit to receive information of all notices of suspicion of terrorist financing and to make proposals to request additional information where necessary. The contact person of the Internal Security Service has the right to exercise supervision specified in the law jointly with the Financial Intelligence Unit. In practice the FIU and the contact person of the Internal Security Service are working in close cooperation. This provision applies also to cooperation regarding suspicion on TF related to NPOs.

1057. The FIU and other relevant authorities have online access to the Non-profit Associations and Foundations Register, the Population Register, etc. – all the registers required for identification of legal or natural persons involved in an NPO. Regular co-operation mechanisms among competent authorities are being used also for NPOs. Furthermore, all the co-operation and information

sharing agreements and tools are also applicable in circumstances where NPOs are involved. Estonian authorities consider since the information on NPOs is publicly available there is no need for specific co-operation agreements concerning this sector. Therefore evaluators note that all the relevant information is available to investigation authorities and there are no provisions that could be considered as obstacles for sharing of information, preventative actions and investigative expertise and capability, with respect to NPO-s suspected of being exploited for terrorist financing purposes.

*Responding to international requests regarding NPO-s – points of contacts and procedures (c.VIII.5)*

1058. Evaluators note that Estonia has mechanisms in place to obtain information on financial activity of non-profit associations and foundations. Authorities have online access to the Non-profit Associations and Foundations Register and may respond to requests.

1059. According to the MLTFPA Art. 37(8) the special point of contact for exchange of information, which include information on NPOs suspected of TF is Estonian FIU, since this provision prescribes FIU's responsibility for organisation of foreign communication and exchange of information.

***Effectiveness and efficiency***

1060. It appears that Estonian authorities have significantly improved framework for preventing the NPOs being abused for TF purposes and the cooperation between FIU and Internal Security Service appears to be very close.

1061. The Non-profit Associations and Foundations Register is a very comprehensive tool which is available on-line to all relevant state authorities. Estonia has a number of registries containing extensive information about ownership and control of legal entities. Access is available to the public and market participants have confirmed the value if this resource in practice. However, no checks are made on the accuracy and validity of information submitted to the register, nor is there supervision of entities' compliance with obligations to keep information up to date and to notify any changes. Authorities rely on the public nature of the registers to identify inaccuracies.

1062. It should be noted that concerning supervision and monitoring of NPOs there is a significant room for progress since the accuracy of the data in the register is not regularly checked and there are limited possibilities for the FIU to organise supervision of NPOs. Therefore authorities should also consider enhancing administrative capabilities of the FIU in this regard

5.2.2 Recommendations and comments

1063. Further outreach should be initiated towards those NPOs that are not members of NENO.

1064. Authorities should consider introducing effective supervision of NPOs and review of reports submitted by NPOs by the Court registry.

1065. Evaluators encourage authorities to conduct periodic reassessments by reviewing new information on the sector's potential vulnerabilities to terrorist activities. In these reassessments all relevant state authorities should be included in order to assist FIU.

5.2.3 Compliance with Special Recommendation VIII

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **SR.VIII** | **LC** | • Absence of effective supervision of NPOs;<br>• Limited outreach to NPOs. |

# 6. NATIONAL AND INTERNATIONAL CO-OPERATION

## 6.1. National co-operation and co-ordination (R. 31 and R. 32)

6.1.1 Description and analysis

***Recommendation 31 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

1066. Estonia was rated "Largely Compliant" for Recommendation 31 in the 3rd round report. The deficiencies underlying the rating were the following: there was no formal cooperation between supervisory authorities (formal agreements, sharing of information) and no formal agreement on cooperation and coordination on supervisory matters.

*Effective mechanisms in place for domestic cooperation and coordination in AML/CFT (c.31.1)*

1067. Estonia has coordination policies involving all relevant competent authorities and the private sector.

1068. According to Order No. 285 of the Government of the Republic of Estonia 11 May 2006, the Government Committee for Coordination of Issues Concerning Prevention of Money Laundering and Terrorist Financing was established. The Chairman of the Government Committee is the Minister of Finance. The Ministry of Finance is responsible for the organisational issues and financing of the Committee. The functions of the Commission include:

- coordinating legislation on prevention of money laundering and terrorist financing and analysing the competence and capacity of the related institutions;
- analysing the implementation of the MLTFPA and coordinating the drafting of new legislation;
- making proposals to the Government of the Republic for the improvement of the measures on prevention of money laundering and terrorist financing and for the amendment of respective legislation;
- co-ordinating international cooperation on the prevention of money laundering and terrorist financing, including coordinating the implementation of respective policy of the EU at the national level.

1069. The Government Committee issues an Activities Report which is submitted to Government once a year (hereinafter Government Committee Activities Report). The Government Committee Activities Report provides a review of actions performed and sets out the action plan for the coming year. The report is approved by the Government. Meetings of the Government Committee are held regularly and at least 4 times a year.

1070. The improvement of collecting relevant statistics in order to carry out adequate analysis and detect possible shortcomings arising from the implementation of the AML/CTF measures is a priority issue for the Government Committee. The effectiveness of the measures in place and further actions for improvement of AML/CTF measures and collecting relevant statistics are evaluated regularly at the meetings of the Government Committee and are also reflected in the Government Committee Activities Report.

1071. The Estonian authorities have stated that the FIU, the FSA and other competent authorities regularly provide an overview of the risk assessments performed on an institutional level at meetings of the Government Committee to ensure concerted action is taken by all relevant authorities to mitigate the risks identified.

1072. Furthermore, the FIU provides updates on money laundering trends and issues regularly to the Government Committee. Annually (mainly at the beginning of the year) the FIU provides a review of actions performed in the previous year and also the main goals and objectives (the action plan) for the coming year. On an annual basis the FIU provides an overview of its activities including new trends and *modus operandi* in money laundering. The FIU also presents topics which need to be addressed – for instance, in 2011 the FIU identified a new threat related to the usage of scrap gold in money laundering schemes. Eventually relevant changes were made to the legislation. On another occasion, the FIU presented an analysis of cash usage in Estonia. The main focus and discussion was on the cash movement over Estonia-Russia border and related risks.

1073. As stated elsewhere in the report, Estonia was at the time of the on-site mission conducting a national risk assessment which required a major coordinated effort by all competent authorities, including the Ministry of Finance, Ministry of Foreign Affairs, Ministry of Interior, Ministry of Justice, FIU, FSA, Internal Security Service, Police, Prosecutor's Office, Tax and Customs Board, the Estonian Banking Association etc. Work was being conducted by five sub-working groups under the supervision of the Ministry of Finance.

1074. As regards cooperation between the FSA and Eesti Pank, the Ministry of Finance and other state agencies in field of legislative drafting, the FSA may submit proposals for the preparation, amendment or repealing of legislation, reviews concerning the activities of the financial sector, and reviews concerning the effect and application of legislation dealing with financial supervision, and to publish such proposals and reviews. If a legal act to be drafted or amended by Eesti Pank, the Ministry of Finance or any other state agency regulates the activities of an entity which is subject to financial supervision or is otherwise related to financial supervision, the draft act shall be coordinated with the FSA. (Art. 49 of the FSA Act)

1075. On the basis of Art. 50 of the FSA Act the FSA concluded a cooperation agreement with the Bank of Estonia and the Ministry of Finance in 2002 to exchange information, to promote attainment of the objectives of financial supervision and make joint contributions to the legislative drafting. In 2006 an additional agreement was concluded in order to regulate cooperation in managing the financial crisis. In addition the evaluators were informed that in 2006 an agreement with the Tallinn Stock Exchange was concluded. Cooperation based on these agreements ensures the smooth functioning of financial markets and regulators and thus prevents possible abuses of the financial system.

1076. On an operational level, national cooperation in the field of AML/CFT has been enhanced by renewed cooperation agreement between Police Board (including FIU), Prosecutors Office and FSA. The agreement provides clearer format for providing expertise in order to improve the prevention, hindering, disclosing the illegal activities and conduct proceedings. The new agreement describes in more detail the instruments of cooperation in the field AML/CFT supervision and exchange of information.

1077. Based on these agreements there have been a number of ad hoc meetings between the counterparts (sometimes even twice in one month). During the meetings the priorities and subsequent actions are set and agreed, but also AML/CFT risks are analysed and mapped out.

1078. As stated in Art. 47(5) of the MLTFPA the FSA, the Board of the Bar Association, the Ministry of Justice and the Chamber of Notaries cooperate with the FIU to ensure proper implementation of the provisions of the MLTFPA. All of these authorities reported having a very good relationship with the FIU.

1079. According to the Estonian authorities, as regards supervision there is almost daily communication between the FIU and the FSA and they meet regularly. In order to improve the cooperation in the field of supervision, the FIU is planning to sign MoU's with Estonian Bar Association and the Chamber of Notaries. Despite strong claims by the authorities, it is doubtful

whether in practice cooperation and coordination between supervisory authorities is sufficient, especially between the FIU, the Bar Association and the Chamber of Notaries. As explained under Recommendation 24, supervision of lawyers and notaries does not appear to be adequately carried out, thereby indicating an absence of a coordinated approach by the authorities to target these categories of reporting entities. Additionally, when requested to provide a breakdown of sanctions imposed by the FIU on credit and financial institutions (some of which may have been subject to FSA supervision) and the nature of the deficiencies identified, neither the FIU nor the FSA could provide the information. This indicates that during the period under review, the FIU may not always have kept the FSA informed of all measures taken for supervisory purposes, even where the institution involved was under the supervision of the FSA.

1080. The Estonian FIU signed cooperation agreements (MoU's) with the following authorities:

- Customs and Tax Board. This MoU regulates the conditions of information exchange between authorities in order to prevent and discover possible ML. Both authorities have appointed contact persons who co-operate daily.
- Internal Security Service in exchange of information regarding FT. The director general of the Internal Security Service has appointed a contact person who co-operates with the Estonian FIU in accordance with Art. 45 of the MLTFPA. The contact person of the Internal Security Service is subject to the Art. 37(1) 1), 6) and 7), Art. 41, Art. 43 (1) to (5) and Art. 44(2) of the MLTFPA. The contact person of the Internal Security Service has the right to exercise supervision specified in Art. 48 of the MLTFPA jointly with the Financial Intelligence Unit.

1081. Estonian authorities confirmed that FIU and ISS have regular communication and meetings in place. Also ISS is sometimes involved in trainings to subjects held by FIU which are related to the terrorism financing prevention.

*Additional element – Mechanisms for consultation between competent authorities and the financial sector and other sectors (including DNFBPS) (c. 31.2)*

1082. The Advisory Committee of Market Participants Of Issues Concerning Prevention Of Money Laundering And Terrorist Financing (hereinafter *Advisory Committee*) was established at the same time with Government Committee and its functions include submission of opinions and proposals to the Committee regarding combating money laundering and terrorism financing. According to the rules of procedure, meetings of the Advisory Committee are also held regularly at least twice a year. The Government Committee nominates the members of the Advisory Committee, who are the representatives of obliged persons under the scope of the MLTFPA. The Advisory Committee's functions include submission of opinions and proposals to the Government Committee regarding combating ML and TF.

1083. The representative of Chamber of Notaries, Estonian Bar Association, Association of Estonian Gambling Organizers, Association of NPOs and Foundations, Chamber of Accountants, Estonian Board of Auditors, Estonian Association of Travel Agencies, Estonian Chamber of Commerce and Industry, also representatives of many associations of financial institutions (i.e. Estonian Banking Association) are members of the Advisory Committee. The representatives of Chamber of Bailiffs and Trustees in Bankruptcy were also invited to join the Committee. Representatives of the FSA and the FIU are customarily present at the meetings. The application of AML/TF measures is regularly discussed, also guidance is provided in cooperation with FSA and FIU at the meetings.

1084. There have been successful initiatives undertaken troughs the Advisory Committee – for example the initiative of the recent amendments in MLTFPA in widening the scope of MLTFPA on precious metal and stones dealers and requesting them to register their activity in Economic Activity Register and relevant Customs Act changes.

***Recommendation 32.1 (Review of the effectiveness of the AML/CFT system on a regular basis)***

1085. The Governmental Committee mentioned above is considered by the Estonian authorities to provide the mechanism for a regular review of the AML/CFT system. As mentioned above statistics are usually discussed and conclusions are always drawn (e.g. as regards SARs), which could be followed by an initiation of the modification of legal provisions. Estonian FIU strategic and operational (case) analysis have been regularly discussed including in the Governmental Committee. It has initiated changes to tax regulations (in order to stop tax frauds and ML with precious metals). Changes in VAT related legislation have been made in several steps.

***Recommendation 30 (Policy makers – resources, professional standards and training)***

1086. The Committee is sufficiently resourced. All of its members are professionally experienced in AML/CFT matters.

***Effectiveness and efficiency***

1087. The cooperation between the competent authorities seems to be active as regards policy cooperation. The law enforcement authorities, including the FIU within its legal confidentiality limits, operate in an open environment of communication and cooperation. A Governmental Committee where all bodies of significance in the AML/CFT domain are represented ensures the coordination between those authorities, besides functioning as a discussion platform and think tank.

1088. Nevertheless, as regards supervision (experience, coordination) further strengthening and formal cooperation or consultation is needed between the supervisory bodies and the FIU (as the supervisory authority). The evaluators welcome the FIU's aim to improve the cooperation in the field of supervision. The evaluators were informed that the FIU has initiated a process to sign MoUs with the Estonian Bar Association and the Chamber of Notaries.

1089. The supervisory authorities, as well as the professional associations and the service providers have a variety of mechanisms in place to facilitate the cooperation and the formal/informal information exchange. In the course of the evaluation none of the supervisory authorities or service providers mentioned any deficiencies or problems regarding the cooperation and information exchange, so it appeared that the system works effectively.

1090. The FSA plays an active role in the Governmental Committee as well as the Advisory Committee of Market Participants.

### 6.1.2 Recommendations and Comments

***Recommendation 31***

1091. Although the cooperation between the relevant bodies appears to be working effectively in practice, it is recommended for all supervisory authorities to consider signing formal agreements for cooperation and coordination on *supervisory matters*. This should translate into more systematic national cooperation and coordination between all supervisory authorities in the AML/CFT field.

### 6.1.3 Compliance with Recommendation 31

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.31** | **LC** | • Insufficient cooperation and coordination between supervisory authorities. |

## 6.2. The Conventions and United Nations Special Resolutions (R. 35 and SR.I)

6.2.1 Description and analysis

***Recommendation 35 (rated LC in the 3rd round report) &Special Recommendation I (rated PC in the 3rd round report)***

1092. Recommendation 35 was rated LC in the 3rd round based on the following conclusions:

*Implementation of the Palermo and Vienna Conventions*

- There are doubts as to whether a conviction or at least indictment for the predicate offence is a prerequisite for a money laundering conviction.

*Implementation of the Terrorist Financing Convention*

- No criminalisation of the financing of an individual terrorist;
- The terrorist financing offence does not cover "collection of funds";
- No specific criminalisation of the collection or provision of funds in the knowledge that they are to be used for any purpose by a terrorist organisation or an individual terrorist.

1093. Special Recommendation I was rated PC in the 3rd round based on the following conclusions:

- Lack of a national mechanism to freeze the funds of EU internals;
- Limited scope of the definition of funds in the EU Regulations, which does not explicitly cover funds owned 'directly or indirectly' by designated persons or those controlled directly or indirectly by designated persons;
- Lack of established national procedure for the purpose of considering delisting requests.

*Ratification of AML Related UN Conventions (c. R.35.1 and of CFT Related UN Conventions (c. SR I.1)*

1094. Estonia has ratified the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention). Reservations have been expressed earlier in respect of the coverage in domestic law of all the physical aspects of the money laundering offence and also in respect of SR.II.

*Implementation of Vienna Convention (Art. 3-11, 15, 17 & 19, c. 35.1)*

1095. Estonian legislation complies with many provisions of the Vienna Convention (See Annex 5 for further information).

1096. The language in Art. 4 of MLTFPA does not clearly replicate the language of the Convention and does not cover purposive elements of concealing and disguising the illicit origin of the property, which narrows the scope of use in self-laundering cases.

1097. Confiscation and seizing measures are available for all offenses under the Convention and the power of law enforcement agencies to identity and trace property that is or may become subject to confiscation is generally not hindered by financial secrecy.

1098. Estonia may provide a number of different types of mutual legal assistance with respect to drug-related ML offenses.

*Implementation of Palermo Convention (Art. 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c.35.1)*

1099. Estonian legislation complies with many provisions of the Palermo Convention (See Annex 5 for further information).

1100. ML offence is not fully in line with the Art. 6 of the Palermo Convention (subject to the shortcomings described under Section 2.1). Confiscation and seizing measures in relation to proceeds obtained through the offenses described by the Convention or property the value of which corresponds to that of such proceeds are available.

1101. Estonia may also provide a wide range of different types of mutual legal assistance with respect to ML offenses involving transnational organized crime. Assistance in searching or seizing for property or evidence in relation to such offenses may be granted.

1102. Preventive measures and supervisory regime are in place for banks and non-bank financial institutions.

1103. Estonia has established the FIU and applied the EU's cross border declaration system.

*Implementation of the Terrorist Financing Convention (Art. 2-18, c.35.1 & c. SR. I.1)*

1104. Estonian legislation complies with many provisions of the TF Convention (See Annex 5 for further information). However, there are several deficiencies as described under SR.II of this Report, e.g. the collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist is not unequivocally covered.

1105. Furthermore, the FT offence does not fully criminalise the financing of all terrorist acts required by the FT convention in its Art. 2(1)(a) since these acts are not criminalised in the PC. Also, for conducts addressed in the specific UN terrorist conventions referred to by Art. 2 of the TF Convention which are covered by Art. 237, an additional purposive element is required which limits the application of TF offence. TF offence does not cover all situations where financing referred to a terrorist act committed abroad. These deficiencies represent factors underlying the rating of SR II, which in some cases go beyond the findings of the 3rd round evaluation team, and consequently provide the basis for downgrading the 3rd round rating.

*Implementation of UNSCRs relating to Prevention and Suppression (c. SR.I.2)*

1106. Estonia has implemented UNSCR 1267 and UNSCR 1373 under European Union legislation (subject to the shortcomings described under Section 2.4) (See Annex 6). With respect to UNSCR 1373, Estonia has provided the United Nations' Counter-Terrorism Executive Directorate (CTED) with 7 periodical reports describing its implementation efforts. United Nations' Resolutions 1267 and 1373 (in respect of Non-European Union citizens) are legally implemented through European Union mechanisms. These lists are circulated to the obligated entities. With the enactment of ISA, Estonia introduced a legal mechanism, which would cover designations in respect of European Union citizens or named persons not covered by the European Union clearing house list proposed by other countries. However, this mechanism still needs to be implemented. No terrorist accounts had been identified. The deficiencies identified under SR.III are relevant in the context of this criterion.

*Additional element – Ratification or Implementation of other relevant international conventions*

1107. The 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime was ratified and entered into force for Estonia in September 2000. Estonia has signed, but not ratified the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the Warsaw Convention). The Convention was signed by Estonia in March 2013.

6.2.1 Recommendations and comments

1108. Estonia has ratified the Vienna and Palermo Conventions and the Terrorist Financing Convention. Since the last round of MONEYVAL evaluations, the domestic legislation has been amended, however, the existing legislation does not fully cover requirements under Recommendations 1 and 3 and Special Recommendation II. Therefore, it is recommended that

Estonia should take necessary measures to remedy identified deficiencies under Recommendations 1 and 3 and Special Recommendation II to fully implement the Vienna, Palermo and TF Conventions.

1109. In addition, the Estonian authorities should also take steps to address the deficiencies identified under SR.III to fully implement the requirements of the UNSCRs.

6.2.2 Compliance with Recommendation 35 and Special Recommendation I

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.35** | **PC** | *Vienna and Palermo Conventions*<br>• The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions, in particular purposive elements of concealing and disguising the illicit origin of the property narrows the scope of use in self-laundering cases (R.1);<br>*Convention for the Suppression of the Financing of Terrorism*<br>• The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered (SR.II);<br>• The TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Art. 2 (1) (a) since these acts are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Art. 237, an additional purposive element is required which limits the application of TF offence;<br>• TF offence does not cover all situations where a person finances a terrorist act committed abroad;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for under Estonian law (R.3);<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property (R.3). |
| **SR.I** | **PC** | *Convention for the Suppression of the Financing of Terrorism*<br>• The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered (SR.II);<br>• The TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Art. 2 (1) (a) since these acts are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Art. 237, an additional purposive element is required which limits the application of TF |

| | | |
|---|---|---|
| | | offence;<br>• TF offence does not cover all situations where a person finances a terrorist act committed abroad;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for under Estonian law (R.3);<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property (R.3);<br>• Deficiencies under SR.III. |

## 6.3. Mutual legal assistance (R. 36, SR. V)

6.3.1 Description and analysis

***Recommendation 36 (rated LC in the 3rd round report)***

1110. Recommendation 36 was rated LC in the 3rd round based on the following conclusions:

- The shortcomings of the money laundering and the terrorist financing offence may limit mutual legal assistance based on dual criminality.

*Legal framework*

1111. International judicial co-operation in criminal matters is described in Chapter 19 of the CCP. Art. 433 CCP sets out the areas in criminal procedure which are subject to international co-operation: extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of judgments of foreign courts, taking over and transfer of criminal proceedings commenced, co-operation with the International Criminal Court and extradition to member states of the European Union. The provisions of Chapter 19 CCP apply unless otherwise prescribed by the international agreements entered into by the Republic of Estonia, European Union legislation or generally recognised principles of international law.

1112. Mutual legal assistance may also be afforded under the provisions of certain conventions and treaties on mutual legal assistance. Estonia ratified the CoE Convention on Mutual Assistance in criminal Matters (CETS No. 30 (1959)) (including its two additional protocols: CETS No. 99 and 182), the CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CETS No. 141 (1990))[70] and the EU Convention on Mutual Assistance in criminal matters between EU Member States (MLA 2000). Furthermore, Estonia has signed bilateral agreements on judicial co-operation with the Russian Federation and Ukraine. Estonia has general judicial co-operation agreements signed with Latvia, Lithuania and Poland. Furthermore, Estonia has judicial co-operation agreements with Russia, Latvia, Lithuania, Ukraine and Poland. Estonia has intergovernmental judicial co-operation agreements with Finland, China, Belarus, Kazakhstan and Moldova. With other EU member states, Estonia mainly cooperates on the basis of EU and CoE instruments. Extradition within EU is based on the Framework Decision on European Arrest Warrant and the surrender of persons. Estonia also has an MLA agreement and extradition agreement with the United States of America.

*Widest possible range of mutual assistance (c.36.1)*

1113. Article 433 CCP sets out mutual assistance between states in criminal matters as one of the areas in criminal procedure which are subject to international co-operation. International co-

[70] Estonia has signed, but not ratified, the CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198 (2005)).

operation in criminal procedure is undertaken pursuant to the provisions of CCP in so far as this is not in conflict with the provisions of the Chapter 19 (international co-operation in criminal procedure). It is possible to conduct proceedings under elements (a) to (f) under c.36.1. on the basis of the request for mutual legal assistance in criminal matters as long as it is not contrary to the provisions of Art. 436(1) of CCP prescribing situations where mutual legal assistance shall not be provided.

1114. It appears that Estonia is able to provide a wide range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings, including assistance in the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; the taking of evidence or statements from persons; providing originals or copies of relevant documents and records as well as any other information and evidentiary items, effecting service of judicial documents; facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country and identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offences, and assets of corresponding value.

*Provision of assistance in timely, constructive and effective manner (c. 36.1.1)*

1115. From the statistics and the information provided by the authorities on time necessary to respond to MLA requests or the statistics on confiscation and seizure on the basis of foreign MLA requests, it appears that Estonia is able to provide such assistance in a timely, constructive and effective manner. Authorities indicated that the average time for execution on foreign requests in Estonia was: 2009- 67 days, 2010- 74 days, 2011- 60 days, 2012 - 65 days, 2013 – 42 days. Furthermore, from the responses provided by other MONEYVAL countries on Estonia's international cooperation it is possible to conclude that these requirements are fulfilled and that Estonia is able to provide such assistance in a timely, constructive and effective manner.

*Mutual legal assistance (36.2)*

1116. Mutual legal assistance is subject to a number of conditions set out under Art. 436(1) of CCP. Mutual legal assistance shall not be provided where:

- it may endanger the security, public order or other essential interests of the Republic of Estonia;
- it is in conflict with the general principles of Estonian law;
- there is reason to believe that the assistance is requested for the purpose of bringing charges against or punishing a person on account of his or her race, nationality or religious or political beliefs, or if the situation of the person may deteriorate for any of such reasons.

1117. Additionally, Art. 436(2) states that a request by a foreign authority to summon a witness or expert shall not be entertained if the requesting state fails to ensure compliance with the requirement of immunity as set out under Art. 465[71] of the CCP.

[71] **Article 465. Immunity of person arriving in Estonia on basis of request for assistance submitted to foreign state**

(1) A witness or expert appearing before a judicial authority on a summons set out in a request for assistance shall not be prosecuted, accused, taken into custody or detained as a suspect in connection with any criminal offence which was committed before his or her departure from the territory of the requesting party and which was not expressly specified in the summons.

(2) The accused appearing before a judicial authority on a summons set out in a request shall not be prosecuted, accused, taken into custody or detained as a suspect in connection with any criminal offences or charges which

1118. These grounds for refusal are not deemed to be unreasonable, disproportionate or unduly restrictive by the evaluation team. Concerning the refusal of execution of one request in 2010, the authorities informed the evaluation team that the reason for refusal was statute of limitations**.**

1119. Article 436(1¹) and (1²) specify that requests for assistance shall not be refused on the grounds that the offence is regarded as a political offence (unless otherwise provided by law or an international agreement) or that the same tax or duty is not imposed or the same taxes, customs or exchange agreements have not been established in Estonia.

1120. None of the conditions mentioned under c.36.2 as examples apply to requests for mutual legal assistance made to Estonian authorities. However, as mentioned in the 3rd round report of Estonia (paragraph 876), in a declaration pursuant to Art. 23 paragraph 1 and Art. 2 of the CoE Convention on Mutual Assistance in criminal Matters (CETS No. 30), Estonia reserved the right to refuse her assistance in case the request concerns an act which is not considered an offence under Estonian laws. This is of significance with respect to the FT offence which is not compliant with the criteria set out under SR II. Estonia may therefore be unable to process a MLA request related to FT.

*Clear and efficient processes (c. 36.3)*

1121. According to Art. 435(1) of the CCP the central authority for international co-operation in criminal procedure is the Ministry of Justice. Section (2) of the same article provides that Courts, Prosecutors' Offices, Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Competition Board and the Military Police are the judicial authorities competent to engage in international co-operation in criminal procedure to the extent provided by law.

1122. When receiving a request for assistance from a foreign state (Art 462 CCP) the Ministry of Justice verifies whether a request received meets the requirements. A request in compliance with the requirements is immediately sent to the Public Prosecutor's Office. The Public Prosecutor's Office verifies whether compliance with the request is admissible and possible and forwards the request to the competent judicial authority for execution.

1123. Requirements for requests for assistance (Art 460) are prescribed concerning the content of the request (the name of the authority making the request, the content of the request, the name, address and, if possible, other contact details of the person with regard to whom the request is submitted, and the facts relating to and the legal assessment of the criminal offence concerning which the request is submitted).

1124. In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may be complied with the consent of the Public Prosecutor's Office before the request for assistance is received by the Ministry of Justice. If a request for assistance is submitted through Eurojust, Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and forward the request to the Estonian competent judicial authority for execution.

---

were committed or brought before his or her departure from the territory of the requesting party and were not expressly specified in the summons.

(3) The immunity provided for in subsections (1) and (2) of this section ceases when the witness, expert or accused has been in Estonia for fifteen consecutive days after the date when his or her presence was no longer required by the judicial authority although he or she has had the opportunity of leaving or, having left, has returned.

1125. Requests for assistance are complied with in accordance with CCP (Art 463 CCP). At the request of a foreign state, a request may be even complied with pursuant to procedural provisions different from the provisions of CCP unless this is contrary to the principles of Estonian law.

1126. These provisions are supplemented by an internal methodology which sets out an efficient mechanism for dealing with and executing MLA requests in a timely way and without undue delays. In particular, the methodology requires the execution of MLA requests without any delay and requires the prosecutor in charge to establish timelines for each individual request according to the circumstances of the case. This methodology has been circulated to all prosecutors. The average time for replying to MLA requests in the period under review was 45 days. On average, MLA requests sent out by Estonia were replied to within 95 days. For every MLA request received, one state prosecutor is in charge of monitoring the request to ensure the quality and timeliness of the execution of the request. From the responses provided by other MONEYVAL countries on Estonia's international cooperation it is possible to conclude that these requirements are fulfilled and that Estonia is able to provide such assistance in a timely, constructive and effective manner.

*Provision of assistance regardless of possible involvement of fiscal matters (c. 36.4)*

1127. There is nothing in the law which restricts cooperation on the basis that the offence is considered to involve fiscal matters. Article 436 ($1^2$) states that the Republic of Estonia shall not refuse to engage in international co-operation 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.

*Provision of assistance regardless of existence of secrecy and confidentiality laws (c. 36.5)*

1128. As concluded under Recommendation 4, the provisions of secrecy and confidentiality laws do not apply to courts, prosecutors and other investigative bodies.

*Availability of powers of competent authorities (applying R.28, c. 36.6)*

1129. All the powers linked with criminal investigation, required under R.28 are available for use in response to requests for mutual legal assistance. As provided under Art. 433 (3), international co-operation in criminal procedure shall be provided pursuant to the provisions of the other chapters of the CCP in so far as this is not in conflict with the provisions of the Chapter 19 (International cooperation in criminal procedure) (In the 3rd round MER, Recommendation 28 was found to be fully Compliant).

*Avoiding conflicts of jurisdiction (c. 36.7)*

1130. Division 4 of Chapter 19 of the CCP regulates transfer and taking over of criminal proceedings. Transfer of a criminal proceeding (Art 474 CCP) initiated with regard to a person suspected or accused of a criminal offence to a foreign state may be requested if:

- the person is a citizen of or permanently lives in the foreign state;
- the person is serving a sentence of imprisonment in the foreign state;
- criminal proceedings concerning the same or any other criminal offence have been initiated with regard to the person in the requested state;
- the evidence or the most relevant pieces of evidence are located in the foreign state;
- it is considered that the presence of the accused at the time of the hearing of the criminal matter cannot be ensured and his or her presence for the purposes of the hearing of the criminal matter is ensured in the requested state.

1131. Art 475 CCP regulates taking over of criminal proceedings in a way that the Ministry of Justice shall forward a request to take over a criminal proceeding from a foreign state to the Public Prosecutor's Office who shall decide whether to take over the criminal proceeding. In addition to the cases provided for in Art. 436 of CCP, acceptance of a request to take over a criminal proceeding may be refused in full or in part if:

- the suspect or accused is not an Estonian citizen or does not live permanently in Estonia;
- the criminal offence concerning which the request to take over the criminal proceeding is submitted is a political offence or a military offence within the meaning of the provisions of the European Convention on Extradition and the Additional Protocols thereto;
- the criminal offence was committed outside the territory of the requesting state;
- the request is in conflict with the principles of Estonian criminal procedure.

*Additional element – Availability of powers of competent authorities required under R. 28 (c. 36.8)*

1132. Authorities indicated that the use of powers mentioned in R.28 is not limited and all the competences may be exercised following due process also when foreign judicial or law enforcement authorities have directly contacted Estonian counterparts. Article 6 of Mutual Legal Assistance Treaty 2000 (MLAT 2000), to which Estonia is a member, foresees direct contacts between competent authorities. However it remains unclear what is the legal basis for direct cooperation with law enforcement counterparts from states that are not state parties to the MLAT 2000. If the country is not a member of MLAT 2000, then the legal basis is the 1959 Convention (Art. 15 section 2 and 4 allows to communicate directly).

***Special Recommendation V (rated LC in the 3rd round report)***

1133. Special Recommendation V was rated LC in the 3rd round based on the following conclusions:

a. The shortcomings of the domestic legislation intended to cover the financing of terrorism may limit mutual legal assistance based on dual criminality.

***International Co-operation under SR. V (applying 36.1 – 36.6 in R.36, c.V.1)***

1134. The analysis under Recommendation 36 applies equally to ML and TF conduct, yet as mentioned in the analysis of c 36.2, the shortcomings of the domestic legislation intended to cover the financing of terrorism may limit mutual legal assistance based on dual criminality.

*Additional element under SR V (applying c. 36.7 & 36.8 in R. 36, c.V.6)*

1135. The analysis under Recommendation 36 applies equally to ML and TF conduct.

***Recommendation 32 (Statistics – c. 32.2)***

1136. The authorities provided the following statistics concerning mutual legal assistance:

**Table 27: MLA requests sent and received by Estonian authorities (MLA requests related only for ML and TF, without connection to predicate offence).**

**Money laundering**

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|
| MLA received | 6 | 5 | 35 | 36 | 34 | 51 | 46 | 33 | 47 |
| MLA sent | 0 | 2 | 4 | 31 | 20 | 15 | 24 | 41 | 22 |

**Terrorist financing**

| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|
| MLA received | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| MLA sent | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 28: Mutual Legal Assistance related to ML (requests sent) broken down by predicate offences**

| | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|
| Computer fraud | 6 | 7 | 8 | 20 |
| Fraud | 1 | 2 | 3 | 10 |
| Tax evasion | 1 | 0 | 0 | 1 |
| Embezzlement | 0 | 0 | 2 | 0 |
| Counterfeiting of Payment Means | 0 | 0 | 2 | 0 |
| Illegal economic activities | 0 | 0 | 0 | 4 |
| Not specified | 12 | 6 | 9 | 7 |
| Total | 20 | 15 | 24 | 42 |

**Table 29: Mutual Legal Assistance related to ML (requests received) broken down by predicate offences**

| | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|
| Computer fraud | 0 | 1 | 16 | 3 |
| Fraud | 4 | 10 | 10 | 7 |
| Tax evasion | 5 | 3 | 9 | 12 |
| Embezzlement | 0 | 0 | 0 | 0 |
| Counterfeiting of Payment Means | 0 | 0 | 0 | 0 |
| Illegal economic activities | 0 | 0 | 0 | 0 |

| | | | | |
|---|---|---|---|---|
| Violation of procedure for handling tobacco product | 0 | 3 | 0 | 0 |
| Violation of procedure for handling tobacco products and tax evasion | 4 | 0 | 0 | 0 |
| Theft | 0 | 1 | 0 | 0 |
| Drug-related crimes | 0 | 7 | 4 | 2 |
| Bankruptcy crime | 0 | 1 | 0 | 0 |
| Abuse of office | 0 | 2 | 0 | 0 |
| Criminal organisation | 0 | 0 | 1 | 0 |
| Bribery | 0 | 0 | 0 | 2 |
| Not specified | 21 | 24 | 11 | 12 |
| Total | 34 | 52 | 51 | 38 |

**Table 30: MLA requests sent related to ML in 2009-2012 broken down by countries to which the requests were sent to.**

| **2009** | |
|---|---|
| Netherlands | 1 |
| Latvia | 4 |
| Moldova | 1 |
| Germany | 11 |
| Hungary | 1 |
| Russia | 1 |
| **Total** | **20** |

| **2010** | |
|---|---|
| Cyprus | 1 |
| Latvia | 5 |
| Norway | 1 |

| | |
|---|---|
| Germany | 7 |
| Denmark | 1 |
| **Total** | **15** |

| **2011** | |
|---|---|
| Netherlands | 1 |
| Italy | 1 |
| Lithuania | 1 |
| Latvia | 4 |
| Sweden | 1 |
| Germany | 11 |
| Switzerland | 1 |
| Finland | 1 |
| Russia | 2 |
| Belarus | 1 |
| **Total** | **24** |

| **2012** | |
|---|---|
| Netherlands | 4 |
| England | 2 |
| Cyprus | 1 |
| Lithuania | 2 |
| Latvia | 12 |
| Poland | 2 |
| Germany | 12 |

| | |
|---|---|
| Singapore | 1 |
| Slovakia | 1 |
| Switzerland | 1 |
| Finland | 1 |
| Denmark | 1 |
| Russia | 1 |
| **Total** | **41** |

**Table 31: MLA requests received related to ML in 2009-2012 broken down by countries sending the request**

| **2009** | |
|---|---|
| Belgium | 1 |
| Bulgaria | 1 |
| Spain | 1 |
| Netherlands | 1 |
| Latvia | 4 |
| Poland | 2 |
| Germany | 9 |
| Finland | 13 |
| Switzerland | 1 |
| Ukraine | 1 |
| **Total** | **34** |

| **2010** | |
|---|---|
| Bulgaria | 3 |
| England | 2 |
| Italy | 1 |

| | |
|---|---|
| Lithuania | 1 |
| Latvia | 11 |
| Poland | 2 |
| Germany | 14 |
| Slovakia | 1 |
| Finland | 14 |
| Switzerland | 2 |
| Hungary | 1 |
| **Total** | **52** |

| **2011** | |
|---|---|
| Ireland | 2 |
| England | 1 |
| Lithuania | 2 |
| Latvia | 9 |
| Sweden | 2 |
| Germany | 20 |
| Finland | 13 |
| Russia | 2 |
| **Total** | **51** |

| **2012** | |
|---|---|
| England | 2 |
| Latvia | 11 |
| Poland | 4 |
| France | 1 |

| | |
|---|---|
| Germany | 5 |
| Finland | 14 |
| Russia | 1 |
| **Total** | **38** |

1137. Authorities indicated that it would be possible to manually gather and provide statistics on date of receipt and date of execution of the request, though it would be very time consuming. All statistics are collected by the Public Prosecutor´s Office. The statistics are collected on a daily basis.

1138. Concerning statistics for seizure and confiscation authorities informed evaluators on requests executed by Estonia 2008 - 1 ; 2009 - 5 ; 2010 – 12; 2011- 3 , 2012-22. Furthermore, Estonia issued in 2010 one and 2012 three certificates for seizure of assets in foreign countries, but not in ML or TF cases. On the bases of foreign countries' requests Estonia received in 2011 - 5 requests, 4 of them in ML cases, 2012 – 1 request (in ML case).

1139. Authorities provided statistics on the total number of incoming and outgoing requests received and sent which were executed, pending, refused and indicated that there was only one request related to ML which was refused. This request was sent by Germany and the ground for refusal was that the case had expired according to Estonian laws. In other cases (which were not related to ML) there have been refusals to request on grounds that the case had expired according to Estonian laws or the act was not crime according to Estonian laws.

**Table 32: total number of MLA requests received and sent**

| **MLA requests received** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** |
| 229 | 263 | 234 | 252 | 208 | 318 | **480** | **547** | **561** | **568** | **685** | **707** | **679** |

**MLA requests sent**

| **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 123 | 177 | 236 | 225 | 183 | 168 | **191** | **216** | **264** | **208** | **260** | **305** | **332** |

1140. Statistics show a significant disproportion in requests received and requests sent, since the number of requests received is significantly higher that the number of the requests sent.

**Table 33: total number of MLA requests executed, refused and pending**

| Mutual legal assistance | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Requests sent** | | | | | | | | | | | | | | | | | | |
| | 2007 | | | 2008 | | | 2009 | | | 2010 | | | **2011** | | | **2012** | | |
| | ML | TF | Other | ML | TF | Other | ML | TF | Other | ML | TF | Other | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** |
| **Executed** | 4 | 0 | 191 | 31 | 0 | 223 | 15 | 0 | 165 | 15 | 0 | 234 | **21** | **0** | **257** | **38** | **0** | **257** |
| **Refused** | 0 | 0 | 4 | 0 | 0 | 3 | 0 | 0 | 2 | | 0 | 4 | **1** | **0** | **2** | **0** | **0** | **3** |
| **Pending** | 0 | 0 | 17 | 0 | 0 | 7 | 5 | 0 | 21 | | 0 | 7 | **2** | **0** | **22** | **4** | **0** | **30** |
| **Total** | 4 | 0 | 212 | 31 | 0 | 233 | 20 | 0 | 188 | 15 | 0 | 245 | **24** | **0** | **281** | **42** | **0** | **290** |
| **Requests received** | | | | | | | | | | | | | | | | | | |
| | 2007 | | | 2008 | | | 2009 | | | 2010 | | | **2011** | | | **2012** | | |
| | ML | TF | Other | ML | TF | Other | ML | TF | Other | ML | TF | Other | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** |
| **Executed** | 35 | 0 | 489 | 36 | 0 | 496 | 34 | 0 | 508 | 51 | 0 | 611 | **51** | **0** | **635** | **37** | **0** | **614** |
| **Refused** | 0 | 0 | 23 | 0 | 0 | 29 | 0 | 0 | 26 | 1 | 0 | 22 | **0** | **0** | **21** | **0** | **0** | **27** |
| **Pending** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** | **0** | **1** | **0** | **0** |
| **Total** | 35 | 0 | 512 | 36 | 0 | 525 | 34 | 0 | 534 | 52 | 0 | 633 | **51** | **0** | **656** | **38** | **0** | **641** |

### *Effectiveness and efficiency*

1141. During the onsite visit the evaluators were informed by the Estonian authorities that the average time to execute a MLA request is not too long and they were consequently provided by relevant statistics. The type of assistance requested depends of the case but in most of the cases the requests seek extracts of bank accounts and/or hearing the persons and/or providing the documents.

1142. In period 2009-2011 a number of received requests related to ML was significantly higher than the number of the requests sent abroad, which might be an indication of lack of initiative of competent authorities on using MLA channels or an indication of larger number of criminal cases related to persons and entities in Estonia. However, the authorities indicated that the reason for relatively low number of outgoing requests is due to the fact that it is possible to get information with the help of FIU or banks and therefore mutual legal assistance request is not always needed.

1143. Specific statistics on time necessary to respond to MLA requests or the statistics on confiscation and seizure on the basis of foreign MLA requests and other MLA statistics seem to be very comprehensive, and the effectiveness and efficiency of the competent authorities related to MLA in ML and TF cases appears to be appropriate, which was confirmed also from the responses provided by other MONEYVAL countries on Estonia's international cooperation.

6.3.2 Recommendations and comments

***Recommendation 36***

1144. Estonia can provide a wide range of mutual legal assistance and co-operation. However, the application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence.

***Special Recommendation V***

1145. The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence.

6.3.3 Compliance with Recommendation 36 and Special Recommendation V

| | Rating | Summary of factors relevant to s.6.3. underlying overall rating |
|---|---|---|
| **R.36** | **LC**[72] | • The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence;<br>• Deficiencies identified under R. 3 may restrict the range of mutual legal assistance that can be provided (c36.1(f)). |
| **SR.V** | **LC**[73] | • The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence;<br>• Deficiencies identified under R. 3 may restrict the range of mutual legal assistance that can be provided (c36.1(f)). |

## 6.4. Other Forms of International Co-operation (R. 40 and SR.V)

6.4.1 Description and analysis

***Recommendation 40 (rated C in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

1146. Recommendation 40 was rated Compliant in the 3rd round MER.

*Wide range of international co-operation (c.40.1) Provision of assistance in timely, constructive and effective manner (c.40.1.1); Clear and effective gateways for exchange of information (c.40.2), Spontaneous exchange of information (c. 40.3)*

*FIU*

1147. Art. 46 MLTFPA gives the FIU the right to exchange information and enter into cooperation agreements with counterpart agencies performing the functions of a financial intelligence unit. No further conditions apply, so the FIU is quite free in its cooperative policy. Although legally not

[72] The review of Recommendation 36 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendation 28.

[73] The review of Special Recommendation V has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 37, 38 and 39.

required the FIU has signed 25 MOUs, mostly because it is an obligation for the counterpart. The information exchanges happen directly on request or spontaneously, normally through FIU-net or the Egmont Secure Web, under the Principles of Information Exchange of the Egmont Group. Urgent requests receive an immediate response within 48 hours, otherwise within an average of 30 days.

*Supervisory authorities*

1148. Article 47(6) of the MLTFPA gives the right to the supervisory authorities to exchange information and cooperate with the supervisory authorities of other states as regards the functions as determined in the MLTFPA. The evaluators are not aware of any data or information of international cooperation, except for the FSA.

1149. According to Art. 6 of the FSA Act, one of the main functions of the FSA in fulfilling the objectives of financial supervision is to cooperate with international organisations for financial supervision, foreign financial supervision authorities and the institutions, committees or other competent foreign bodies or persons of the European Union and participate in the activities of the Colleges of Supervisors.

1150. As stated in Art. 47 of the FSA Act, the FSA is empowered to exchange information with its foreign counterparts. The FSA has the right to send and exchange confidential information which is necessary for the performance of its foreign counterparts' functions. Furthermore, the FSA Act stipulates that information sent, received or exchanged in this manner is deemed to be confidential and can be used only for supervisory purposes.

1151. The Estonian FSA has concluded Memoranda of Understanding with the supervisory authorities of Finland, Sweden, Denmark, Germany, Switzerland, the Netherlands, Cyprus, Latvia, Lithuania and Russia. Most of the MoUs contain articles promoting cooperation on money laundering issues. These MoUs allow for prompt and constructive exchange of information between the parties.

1152. The FSA Act provides for the exchange of information with foreign counterparts upon receipt of a reasoned request and, at the same time, allows the provision of spontaneous information at the FSA's initiative. Information exchange with foreign supervisory authority must be based on a cooperation agreement.

1153. The MoUs signed by the FSA with its counterparts allow exchange of information both spontaneously as well as upon request. All MoUs contain, as a rule, a list of contact persons, who can be contacted directly to safeguard the most effective flow of information.

1154. The FSA does not keep statistics concerning the exchange of information with its counterparts. However, as explained by the authorities this information could be obtained manually as it is available in the electronic registry of official correspondence.

1155. The Estonian FIU, in its capacity as a supervisor, is able to exchange information both spontaneously and upon request with foreign supervisors and in relation to money laundering, terrorist financing and the underlying predicate offences. The FIU reported that such exchanges are very unusual.

*Law enforcement authorities*

1156. Outside the context of mutual legal assistance the Estonian Police Board exchanges operational information routinely, at its own initiative or upon request, with foreign police forces, mostly but not necessarily on the basis of cooperation agreements. These contacts normally take place using the Interpol communication channel or within the SIS with Schengen countries.

*Making inquiries on behalf of foreign counterparts (c.40.4) FIU authorised to make inquiries on behalf of foreign counterparts (c. 40.4.1), Conducting of investigation on behalf of foreign counterparts (c. 40.5)*

*FIU*

1157. Any foreign FIU request being considered equal to an SAR (Art. 4(2) Regulation 13) the Estonian FIU is authorised to use all its inquisitive analytical powers domestically at its disposal to collect additional information on request of a counterpart. It can and does search its own and any other database it has access to directly or indirectly as an FIU.

*Supervisory authorities*

1158. The FSA is entitled to use the rights and powers determined in the FSA Act in order to fulfil the request of the European Supervisory Authorities and other counterparts. The request to be fulfilled must be based on a corresponding cooperation agreement or if the information is inevitably necessary for the supervision and does not damage public orders of Estonia. The FSA participates together with the financial supervision authorities of other EEA countries in the applications for authorisations and other financial supervision procedures in the cases specified in the FSA Act and other legislation. More importantly, the FSA may act on behalf of foreign counterparts, based on a corresponding request of a supervisory authority of a contracting state (CrIA Art. 101 (2), Payment Institution Act Art. 97 (2)).

*Law enforcement authorities*

1159. The police cannot start formal investigations on behalf or upon request of a foreign law enforcement authority except in the framework of mutual legal assistance and according to Chapter 19 CCP. It can however collect intelligence in an informal way and give practical assistance.

*No unreasonable or unduly restrictive conditions on exchange of information (c.40.6)*

*FIU*

*1160.* The exchange of information between Estonian FIU and its foreign counterparts occurs on the basis of the internationally accepted Egmont cooperation rules. The exchange is purpose bound and any dissemination is subject to the prior consent of the supplying FIU.

*Supervisory authorities*

1161. Based on the provision of Art. 47 (3)-(6) of the FSA Act, the exchange of information between Estonian FSA and its foreign counterparts is not subject to disproportionate or unduly restrictive conditions and this takes place in accordance with international standards as has been highlighted above.

*Law enforcement authorities*

1162. The police to police cooperation is only limited by the nature of the request, in that it cannot respond to requests that belong in the MLA sphere or requiring coercive measures.

*Provision of assistance regardless of possible involvement of fiscal matters (c.40.7)*

*FIU*

1163. It is completely irrelevant if the request also touches upon possible fiscal aspects as long it is related to money laundering or terrorism financing. Fiscal evasion or frauds are money laundering predicates anyway.

*Supervisory authorities*

*1164.* Due to the requirements of Art. 47 (5) an (6) of the FSA Act requests for cooperation cannot be refused on the sole ground that also fiscal matters are considered

*Law enforcement authorities*

*1165.* A possible fiscal aspect of the requested cooperation does not preclude operational cooperation as long the request relates to criminal matters

*Provision of assistance regardless of existence of secrecy and confidentiality laws (c.40.8)*

*FIU*

1166. The FIU has access to all confidential information or data protected by banking or other secrecy, available in the domestic context, also at request of a counterpart FIU. Exception is made for information covered by legal privilege.

*Supervisory authorities*

1167. The Supervision Authority has the right to communicate confidential information to a foreign financial supervision authority or other competent foreign body or person only if the receiver of the confidential information is obliged to maintain the confidentiality of the information received and the information is necessary for exercising financial supervision. Confidential information may be communicated to the central bank or other competent body of EEA country, if it is necessary for performing its functions, including the information which is necessary for exercising the financial policy, resolving liquidity issues, functioning of the payment and settlement systems and other purposes to ensure the stability of the financial system of this EEA country. Information received as a result of the cooperation may be disclosed if a respective agreement has been entered into with the foreign financial supervision authority or other competent foreign authority or person.

*Law enforcement authorities*

1168. Direct assistance can only be given in matters not regulated by the CCP. Any request for information covered by secrecy or confidentiality rules has to use the MLA channels and procedure.

*Safeguards in use of exchanged information (c.40.9)*

*FIU*

1169. The use of information collected from whatever source is regulated in Art. 43 and 44 MLTFPA, imposing restricted access and strict confidentiality rules. Furthermore the FIU applies the Egmont Group Principles of Information Exchange on any information received from counterpart FIUs, particularly the prior consent and confidentiality rule.

*Supervisory authorities*

1170. Article 54 of the FSA Act provides for controls and safeguards to ensure that information received during supervision is used in a legal and authorised manner.

*Law enforcement authorities*

1171. Police type information obtained from foreign police authorities through direct assistance are protected by the same confidentiality rules as applicable in the domestic context. **.**

*Additional elements – Exchange of information with non-counterparts (c.40.10 and c.40.40.1) Competent authorities pursuant to request from foreign FIU (c.40.11)*

*FIU*

1172. As a rule the Estonian FIU only cooperates with counterpart FIUs (Art. 46 MLTFPA), but in its capacity of supervisory body it can also exchange information with foreign supervisory authorities.

*Supervisory authorities*

*1173.* The evaluators have been informed that if there is a cooperation agreement with non-counterparts the regulation does not exclude the possibility to exchange information. According to Art. 54(4) of the FSA Act confidential information and documents containing information on the results of financial supervision may be disclosed to defined third persons. Information received as a result of the cooperation may be disclosed if a respective agreement has been entered. According to Art. 54($4^1$) the FSA has the right to communicate confidential information to a foreign financial supervision authority or other competent foreign body or person only if the receiver of the confidential information is obliged to maintain the confidentiality of the information received and the information is necessary for exercising financial supervision.

*Law enforcement authorities*

1174. Police only gives assistance to counterpart police authorities.

***Special Recommendation V (rated C in the 3rd round report)***

1175. All comments above equally apply in an FT context.

***Recommendation 32 (Statistics – other requests made or received by the FIU, spontaneous referrals, requests made or received by supervisors)***

1176. The following statistical figures relate to non-MLA related exchanges:

FIU

a. General

In 2010 the FIU received 255 requests from 41 countries and gave the permission to use the information in 246 cases. In 2011 the FIU received 225 requests from 43 countries and gave the permission to use the information in 191 cases. In 2012 the FIU received 228 requests from 36 countries and gave the permission to use the information in 224 cases. Reasons for refusal or non-compliance are unknown.

**Table 34: FIU sent requests**

| **Requests sent** | **2008** | | | **2009** | | | **2010** | | | **2011** | | | **2012** | | | **2013** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ML** | **TF**[74] | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** |
| Executed | 107 | n/a | n/a | 229 | n/a | n/a | 193 | n/a | n/a | 154 | n/a | n/a | 208 | n/a | n/a | 151 | n/a | n/a |
| Denied [75] | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |

[74] All requests are filed under ML suspicion; no separate statistics for TF

[75] Statistics not kept

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pending from previous[76] year(s) | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Other | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| **Total** | 107 | **n/a** | **n/a** | **228** | **n/a** | **n/a** | **193** | **n/a** | **n/a** | **154** | **n/a** | **n/a** | **208** | **n/a** | **n/a** | **151** | **n/a** | **n/a** |

**Table 35: FIU received requests**

| **Requests received** | **2008** | | | **2009** | | | **2010** | | | **2011** | | | **2012** | | | **2013** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **TF** | **Other** | **ML** | **FT** | **Other** |
| Executed | 204 | n/a | n/a | 205 | n/a | n/a | 255 | n/a | n/a | 225 | n/a | n/a | 228 | n/a | n/a | *194* | n/a | n/a |
| Denied | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Pending from previous year(s) | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Other | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| **Total** | 204 | n/a | n/a | 204 | n/a | n/a | 255 | n/a | n/a | 225 | n/a | n/a | 228 | n/a | n/a | *194* | n/a | n/a |

Average response time to incoming requests: 17 days in 2012.

b. Top 5 incoming

| | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| 1 | Latvia | Latvia | Latvia | Latvia | Latvia | Latvia |
| 2 | Finland | Russia | Russia | Finland | Finland | Finland |
| 3 | Taiwan | Finland | Finland | Russia | Russia | Lithuania |

[76] Statistics not kept

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Russia | Ukraine | Lithuania | Lithuania/Ukraine | Lithuania/Ukraine | Russia |
| 5 | Ukraine | Lithuania | Ireland/Cyprus/Ukraine | Lithuania/Ukraine | Lithuania/Ukraine | Moldova |

Top 5 outgoing

| | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| 1 | Latvia | Latvia | Latvia | Latvia | Latvia | Latvia |
| 2 | Russia | Russia | Russia | Russia | Russia | Russia |
| 3 | Finland | Sweden | Lithuania | Belorussia | Sweden | Finland |
| 4 | Sweden | Lithuania/Finland | Sweden | Sweden | Poland | Sweden |
| 5 | UK/Lithuania | Lithuania/Finland | Finland/UK | Luxembourg | Finland | Lithuania/Germany |

c. Spontaneous dissemination to foreign counterparts:

2009 - 34

2010 – 27

2011 – 43

2012 – 18

2013 – 23

2014 (first 5 months) - 21.

2. Police & Customs

1177. The PBGB does not keep non-MLA related statistics in a systematic way.

1178. The ETCB keep general statistics on international exchanges, however not ML/FT specific:

2011 - 73

2012 - 105

2013 - 139

3. Supervisory authorities

1179. No statistics were provided by the supervisory authorities.

***Effectiveness and efficiency***

***Recommendation 40***

*FIU*

1180. FIU to FIU cooperation is frequent and quite satisfactory. No incidents were reported. Comprehensive statistics are kept, although the absence of information about the numbers and the reasons for refusal or non-compliance is a negative factor.

*Supervisory authorities*

1181. International cooperation of the FSA is frequent, according to the authorities. In the absence of statistics, the evaluation team could not determine whether supervisory authorities fulfil the requirements under this Recommendation effectively.

*Law enforcement authorities*

1182. Effectiveness cannot be assessed in the absence of concrete and comprehensive statistical information, although there are no counter-indications.

6.4.2 Recommendation and comments

*FIU + law enforcement*

1183. The statistical data kept by the FIU are generally comprehensive and detailed. They should be complemented by information on the grounds for refusal or non-execution. The other relevant law enforcement authorities should start maintaining ML/FT specific statistics on operational cross-border exchanges.

*Supervisory authorities*

1184. Supervisory authorities should maintain statistics on requests for information.

6.4.3 Compliance with Recommendation 40 and Special Recommendation V

| | Rating | Summary of factors relevant to s.6.5 underlying overall rating |
|---|---|---|
| **R.40** | **LC** | **Effectiveness**<br>• Effectiveness was not demonstrated by law enforcement and supervisory authorities. |
| **SR.V** | **LC** | **Effectiveness**<br>• Effectiveness was not demonstrated by law enforcement and supervisory authorities. |

# 7. OTHER ISSUES

The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report i.e. all of section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report should also contain brief description including the box showing the ratings and the factors underlying the rating.

## 7.1. Resources and Statistics

7.1.1 Description and analysis

***Recommendation 30 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

1185. Recommendation 30 was rated Largely Compliant in the 3rd round report. The following deficiencies were identified:

- The number of supervisory staff at the FIU was insufficient;
- The Police and the Tax and Customs Board did not have enough human and technical resources;
- The supervisory authorities were found not to have sufficient resources.

*FIU*

1186. The FIU's staff was found to be adequate by the evaluation team. The budget and technical resources of the FIU were also deemed to be sufficient. The necessary measures are in place to ensure that FIU employees are of high integrity and have appropriate experience and expertise. They are required to keep confidential for an indefinite period any information received in the course of their functions. The FIU staff regularly receives training at both a domestic and international level.

*Customs Authority*

1187. The Investigation Department of the ETCB was found to have sufficient financial, human and technical resources. ETCB staff are required to comply with an order on ethical behaviour, which order comprises guidance papers governing the integrity of officials and confidentiality of information. Training is provided on a yearly basis.

*Supervisory authorities*

1188. The AML Unit of the Business Conduct Supervision Division of the FSA is adequately staffed and trained. The AML Unit is supported by the other departments of the FSA. The Prudential Supervision of the FSA, which is responsible for market entry and licensing, is also sufficiently staffed. The FSA Act sets out the criteria which have to be met by employees, including necessary education, experience, professional qualifications and an impeccable professional and business reputation. Confidentiality requirements are also provided for, which apply for an indefinite period of time. Training is provided on a regular basis.

1189. The FIU as a supervisor is not adequately staffed. Supervisory activities are conducted by analysts who have other non-supervisory responsibilities. The situation has not changed since the 3rd round. In addition, internal processes for supervision purposes do not appear to be sufficiently streamlined. The same requirements for integrity and confidentiality apply to other staff of the FIU. Training on supervisory matters appears to be adequate.

*Policy makers*

1190. The Government Committee responsible for policy coordination is adequately staffed.

***Recommendation 32 (rated LC in the 3rd round report)***

*Summary of 2008 factors underlying the rating*

1191. Recommendation 32 was rated Largely Compliant in the 3rd round report. The following deficiencies were identified:

- The statistics on MLA were not kept for predicate offences;
- No statistics were made available on the timeliness of extradition procedures;
- No statistics were made available on the exchange of information by the FSA with foreign counterparts.

1192. Overall, statistics maintained by all Estonian authorities are adequate. However, it was noted that, with respect to ML convictions, the Ministry of Justice does not maintain detailed information on convictions such as the underlying predicate offence, whether the latter was committed domestically or abroad, the sentences handed down, the amounts laundered and whether the convictions were for self-laundering, third party ML, stand alone ML and autonomous ML.

1193. The evaluation team also noted that statistics maintained by the ETCB (although not a technical requirement under the FATF Recommendations) do not give an indication of ensuing LE results. Additionally, statistics broken down by the number of cases where cash was restrained following a false declaration, separate from those situations where a suspicion of ML/FT was identified, are not maintained.

1194. The FIU does not maintain statistics on whether a request for information from a foreign FIU has been granted or refused.

1195. As regards, the FIU as a supervisory authority, no statistics were provided on the number of on-site and off-site actions carried out for every category of financial institution under FIU supervision.

1196. The supervisory authorities do not collect statistics on formal (or informal) requests for assistance (made or received), including whether the request was granted or refused.

### 7.1.2 Recommendations and comments

***Recommendation 30***

***1197.*** Staffing, training and structure of the FSA is broadly appropriate. While training and professional standards at the FIU are appropriate, it is not clear that there are sufficient supervision staff at the FIU to adequately supervise the financial institutions for which they are responsible.

***Recommendation 32***

1198. It is strongly recommended that, with respect to ML convictions, the Ministry of Justice maintains additional information such as the underlying predicate offence, whether the latter was committed domestically or abroad, the sentences handed down, the amounts laundered and whether the convictions were for self-laundering, third party ML, stand alone ML and autonomous ML. This will enable the authorities to determine, to a greater extent, whether Recommendation 1 is being implemented effectively.

1199. The ETCB keeps comprehensive statistics, although deplorably these do not give an indication of the ensuing LE results. The ETCB should also consider maintaining separate statistics on the

number of cases where cash was restrained following a false declaration and where there is a suspicion of ML/FT.

1200. The FIU should maintain statistics on whether a request made by another FIU has been granted or refused.

1201. The authorities should collect statistics on formal (and informal) requests for assistance made or received by supervisors, including whether such requests were granted or refused.

1202. The FIU should maintain statistics on on-site inspections broken down by category of financial institution.

7.1.3 Compliance with Recommendations 30 and 32

| | Rating | Summary of factors underlying rating |
|---|---|---|
| **R.30** | **LC** | • Insufficient supervisory staff at the FIU to carry out its functions. |
| **R.32** | **LC** | • Insufficient statistics are kept by the FIU on on-site inspections;<br>• No statistics on whether requests made to the FIU were granted or refused;<br>• No statistics maintained on formal requests for assistance made or received by the supervisors relating to AML/CFT. |

## 7.2. Other Relevant AML/CFT Measures or Issues

## 7.3. General Framework for AML/CFT System (see also section 1.1)

# IV. TABLES

## TABLE 1. RATINGS OF COMPLIANCE WITH FATF RECOMMENDATIONS

The rating of compliance vis-à-vis the FATF 40+ 9 Recommendations is made according to the four levels of compliance mentioned in the AML/CFT assessment Methodology 2004 (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (N/A).

The following table sets out the ratings of Compliance with FATF Recommendations which apply to Estonia. *It includes ratings for FATF Recommendations from the 3rd round evaluation report that were not considered during the 4th assessment visit. These ratings are set out in italics and shaded.*

| Forty Recommendations | Rating | Summary of factors underlying rating[77] |
|---|---|---|
| **Legal systems** | | |
| 1. Money laundering offence | **LC** | • The purposive elements of concealing and disguising the illicit origin of the property narrows the scope of use in self-laundering cases;<br>• The full concept of terrorist financing is not a predicate offence to money laundering;<br>**Effectiveness**<br>• Concerns over evidential thresholds to establish underlying predicate criminality. |
| 2. *Money laundering offence Mental element and corporate liability* | ***C*** | |
| 3. Confiscation and provisional measures | **PC** | • Confiscation of property of corresponding value to instrumentalities is not fully provided for;<br>• Confiscation of property of corresponding value to laundered property is not fully provided for;<br>• Unclear whether confiscation of property can be applied where the owner or possessor has not been identified;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for under Estonian law;<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property; |

[77] These factors are only required to be set out when the rating is less than Compliant.

| | | |
|---|---|---|
| | | • Technical limitations in relation to confiscation of instrumentalities and value confiscation extend to seizure;<br>**Effectiveness**<br>• Low number of confiscation orders with respect to proceeds-generating crime;<br>• Low volume of confiscated assets overall. |
| **Preventive measures** | | |
| 4. Secrecy laws consistent with the Recommendations | **LC** | • Provisions relating to sharing of information between financial institutions where this is required by R.7, R.9 and SR VII, are drafted in a manner that leaves some uncertainty in interpretation.<br>**Effectiveness**<br>• Some uncertainty amongst financial institutions regarding whether sharing of information was permitted on a statutory basis or on the basis of a customer mandate. |
| 5. Customer due diligence | **LC** | • No clear requirement to determine whether the customer is acting on behalf of another person (C.5.5.1);<br>• No requirement to apply CDD requirements to existing customers (c.5.17);<br>**Effectiveness**<br>• Some shortcomings in the identification and verification of beneficial owners (especially on indirect ownership and control) by certain categories of financial institutions;<br>• Some shortcoming in the identification and verification of the source of funds by certain categories of financial institutions. |
| 6. *Politically exposed persons* | ***LC*** | • The MLTFPA exempts from its definition of politically exposed persons such persons who have not performed any prominent public functions for at least a year;<br>• At least one of the smaller local banks, at the time of the on-site visit, did not conduct independent background checks on their customer's possible role as a politically exposed person (in contrast to the larger, internationally active banks which seem to follow their obligations). |

| | | |
|---|---|---|
| 7. *Correspondent banking* | ***LC*** | • There is no specific provision in Estonian law which clearly requires understanding the respondent bank's business;<br>• There is no clear legal requirement to obtain approval from senior management before establishing new correspondent relationships;<br>• The MLTFPA allows to apply simplified CDD measures for correspondent banking relationships with financial institutions of EU member countries (an exception which is not provided for by FATF Recommendation 7);<br>• Financial institutions are only required to detail the banks' obligations in the application of due diligence measures for prevention of money laundering and terrorist financing but not all the respective AML/CFT responsibilities of each institution. |
| 8. New technologies and non face-to-face business | **C** | |
| 9. *Third parties and introducers* | ***LC*** | • There is no clear requirement for obligated persons to ensure that timely reproduction of the necessary documentation from third parties is possible;<br>• Concerning criterion 9.4, there has not been guidance of the Estonian authorities to explain the financial institutions which countries can be considered as having requirements equal to those provided in the MLTFPA in force and can be supposed to comply with Recommendation 9;<br>• It seems that in the exceptional cases provided for by §14 (4) MLTFPA, the ultimate responsibility for customer identification and verification does not remain with the financial institution relying on the third party. |
| 10. Record keeping | **LC** | • No provision in law or regulation to ensure that the mandatory record-keeping period may be extended in specific cases upon request of competent authorities (as preventive measures). |
| 11. Unusual transactions | **PC** | • The requirement to pay special attention to complex, unusual large transactions does not apply to "patterns of transactions" as required by the criterion;<br>• The requirement to pay special attention does not |

| | | |
|---|---|---|
| | | apply to transactions which have "no apparent or visible lawful purpose" as required by the criterion;<br>• No clear requirement to examine the nature, purpose or background when discovering a complex or unusual transaction during transaction monitoring;<br>• No clear obligation to keep records of findings that do not lead to STR. |
| 12. DNFBPS – R.5, 6, 8-11[78] | **PC** | ***Applying Recommendation 5***<br>• No clear requirement to determine whether the customer is acting on behalf of another person;<br>• No requirement to apply CDD requirements to existing customers;<br>**Effectiveness**<br>• Weakness in the implementation of the identification and verification of source of funds, especially in case of higher risk customers and PEPs;<br>• Some shortcomings in the implementation of risk-based approach (extent of CDD measures);<br>• Weakness in the implementation of CDD measures by real estate agents;<br>• Some deficiencies in the implementation of CDD measures of dealers in precious metals and dealers in precious stones.<br>***Applying Recommendation 10***<br>• No provision in law or regulation to ensure that the mandatory record-keeping period may be extended in specific cases upon request of competent authorities (as preventive measures).<br>**Effectiveness**<br>• Lack of effective implementation of the record-keeping requirements with regard to real estate agents.<br>***Applying Recommendation 11***<br>• The requirement to pay special attention to complex, unusual large transactions does not |

[78] The review of Recommendation 12 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 6 and 9.

| | | |
|---|---|---|
| | | apply to "patterns of transactions" as required by the criterion;<br>• The requirement to pay special attention does not apply to transactions which have "no apparent or visible lawful purpose" as required by the criterion;<br>• No clear requirement to examine the nature, purpose or background when discovering a complex or unusual transaction during transaction monitoring;<br>• No clear obligation to keep records of findings that do not lead to STR. |
| 13. Suspicious transaction reporting | **LC** | • No explicit requirement to report suspicions on funds linked or related to, terrorism, terrorist acts or by terrorist organisations;<br>**Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness. |
| 14. *Protection and no tipping-off* | ***C*** | |
| 15. *Internal controls, compliance and audit* | ***LC*** | • The absence of supplementary Regulation by the Ministry of Finance under the new act on details of the internal controls and procedures causes some uncertainty regarding the completeness of Estonian financial institutions' internal rules of procedure concerning AML/CFT issues which, at the time of on-site visit, were based on a Regulation of the Minister of Finance issued under the previous law;<br>• Financial institutions are not required to have guidance in their internal rules concerning the detection of unusual and suspicious transactions;<br>• Limited requirements concerning screening procedures for new employees;<br>• Financial institutions are not required to include in their training of employees current AML/CFT techniques methods and trends. |
| 16. DNFBPS – R.13-15 & 21[79] | **PC** | *Applying Recommendation 13* |

[79] The review of Recommendation 16 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 14, 15 and 21.

| | | |
|---|---|---|
| | | • No requirement to report suspicions on funds linked or related to, or to be used for, terrorism, terrorist acts or by terrorist organisations or those who finance terrorism;<br>**Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness;<br>• Underreporting by certain DNFBPs.<br>*Applying Recommendation 21*<br>• Technical deficiency in relation to the application of the obligation to a customer or person from one of the stipulated countries;<br>• 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;<br>• No clear requirement to keep records of findings that do not lead to STR;<br>**Effectiveness**<br>• No awareness-raising by the authorities to DNFBPs on jurisdictions which do not or insufficiently apply FATF Recommendations;<br>• Weak awareness of this requirement by certain DNFBPs. |
| 17. Sanctions | **PC** | • Range of available sanctions is neither effective nor proportionate for certain categories of financial institutions;<br>• Maximum financial penalties do not appear dissuasive;<br>• Sanctions available for legal persons that are financial institutions are not available for their directors and senior management;<br>**Effectiveness**<br>• Narrow range of sanctions applied in practice. |
| 18. *Shell banks* | ***LC*** | • The CrIA does not clearly prohibit the establishment or continuous operation of shell banks in Estonia which are operated outside from the European Economic Area (EEA). |
| 19. *Other forms of reporting* | ***C*** | |

| | | |
|---|---|---|
| 20. *Other DNFBPS and secure transaction techniques* | ***C*** | |
| 21. Special attention for higher risk countries | **PC** | • Technical deficiency in relation to the application of the obligation to a customer or person *from* one of the stipulated countries;<br>• 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;<br>• No clear requirement to keep records of findings that do not lead to STR;<br>**Effectiveness**<br>• Circular letters not distributed to all financial institutions. |
| 22. *Foreign branches and subsidiaries* | ***LC*** | • No specific requirement on the financial institutions to require the application of AML/CFT measures to foreign branches and subsidiaries beyond customer identification and record keeping;<br>• There is no requirement to pay special attention to situations where branches and subsidiaries are based in countries that do not or insufficiently apply FATF Recommendations;<br>• The MLTFPA does not explicitly require branches and subsidiaries in host countries to apply, when the minimum AML/CFT requirements of the home and host countries differ, the higher standard to the extent that local laws or regulations differ. |
| 23. Regulation, supervision and monitoring | **LC** | **Effectiveness**<br>• Insufficient ongoing supervision and monitoring of investment firms, life insurance companies and payment service providers;<br>• Effectiveness issues for the FIU - low number of staff, low levels of on-site inspections, decreasing levels of off-site supervision, no proper internal methodology for conducting on-site inspections. |
| 24. DNFBPS - Regulation, supervision and monitoring | **PC** | • Sanctions available for legal persons that are financial institutions do not extend to directors and senior management;<br>**Effectiveness** |

| | | |
|---|---|---|
| | | • Insufficient supervisory resources at the FIU;<br>• In practice only misdemeanour proceedings are used by FIU;<br>• Low level of on-site visits for certain DNFBPs under FIU supervision;<br>• Insufficient supervision undertaken by the Bar Association and Chamber of Notaries;<br>• No sanctions imposed by either the Bar Association or Chamber of Notaries. |
| 25. Guidelines and Feedback | **C** | |
| **Institutional and other measures** | | |
| 26. The FIU | **LC** | • Insufficient power to query all relevant additional information from lawyers;<br>• Confidentiality risk when querying unregulated persons. |
| 27. *Law enforcement authorities* | ***C*** | |
| 28. *Powers of competent authorities* | ***C*** | |
| 29. Supervisors | **LC** | • No adequate sanctioning power against directors and senior management for breaches by a financial institution. |
| 30. Resources, integrity and training[80] | **LC** | • Insufficient supervisory staff at the FIU to carry out its functions. |
| 31. National co-operation | **LC** | • Insufficient cooperation and coordination between supervisory authorities. |
| 32. Statistics[81] | **LC** | • Insufficient statistics are kept by the FIU on on-site inspections;<br>• No statistics on whether requests made to the FIU were granted or refused; |

[80] The review of Recommendation 30 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on resources integrity and training of law enforcement authorities and prosecution agencies.

[81] The review of Recommendation 32 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 12, 16, 20, 27, 29, 38 and 39 and Special Recommendation IX.

| | | |
|---|---|---|
| | | • No statistics maintained on formal requests for assistance made or received by the supervisors relating to AML/CFT. |
| 33. Legal persons – beneficial owners | **PC** | • There is limited control over the obligations of legal persons to submit updated information on ownership and control to the register;<br>• Maintenance of share registers and shareholder registers by limited companies is not supervised;<br>• The legal framework does not ensure that information held in the Commercial Register is adequate, accurate and timely;<br>• It is doubtful whether competent authorities are in a position to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons. |
| 34. Legal arrangements – beneficial owners | **NA** | |
| **International Co-operation** | | |
| 35. Conventions | **PC** | *Vienna and Palermo Conventions*<br>• The physical elements of money laundering offence do not fully correspond to the Vienna and Palermo Conventions, in particular purposive elements of concealing and disguising the illicit origin of the property narrows the scope of use in self-laundering cases (R.1);<br>*Convention for the Suppression of the Financing of Terrorism*<br>• The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered (SR.II);<br>• The TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Article 2 (1) (a) since these acts are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Article 237, an additional purposive element is required which limits the application of TF offence;; |

| | | |
|---|---|---|
| | | • TF offence does not cover all situations where a person finances a terrorist act committed abroad;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for under Estonian law (R.3);<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property (R.3). |
| 36. Mutual legal assistance (MLA)[82] | **LC** | • The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence;<br>• Deficiencies identified under R. 3 may restrict the range of mutual legal assistance that can be provided (c.36.1(f)). |
| 37. *Dual criminality* | ***LC*** | • Requirement of dual criminality contained in the reservation to the CETS Convention 30 may impede effectiveness of the mutual legal assistance in money laundering and terrorist financing cases;<br>• Because of the gaps in the domestic legislation concerning the coverage of financing of terrorism and money laundering, the requirement of dual criminality for extradition would mean that not all kinds of terrorist financing and money laundering offences would be extraditable. |
| 38. *MLA on confiscation and freezing* | ***LC*** | • No arrangements for coordinating seizure and confiscation action with other countries are established;<br>• Establishment of an asset forfeiture fund was not considered;<br>• No sharing of confiscated assets with other countries when confiscation is a result of coordinated law enforcement action is applied. |
| 39. *Extradition* | ***LC*** | • There are no explicit provisions in Estonian legislation which would require in case of refusal to extradite an Estonian national to submit the case without undue delay to the competent Estonian authorities for the purpose of prosecution of the offences set forth in the extradition request; |

[82] The review of Recommendation 36 has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendation 28.

| | | |
|---|---|---|
| | | • In the absence of detailed statistics it is not possible to determine whether extradition requests are handled without undue delay. |
| 40. Other forms of co-operation | **LC** | **<u>Effectiveness</u>**<br>• Effectiveness was not demonstrated by law enforcement and supervisory authorities. |
| **Nine Special Recommendations** | | |
| SR.I Implement UN instruments | **PC** | *Convention for the Suppression of the Financing of Terrorism*<br>• The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered (SR.II);<br>• The TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Article 2 (1) (a) since these acts are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Article 237, an additional purposive element is required which limits the application of TF offence;<br>• TF offence does not cover all situations where a person finances a terrorist act committed abroad;<br>• The confiscation of instrumentalities intended to be used in the commission of financing of terrorism offence is not fully provided for under Estonian law (R.3);<br>• The deficiency identified in the criminalisation of the FT may limit the ability to freeze and confiscate property (R.3);<br>• Deficiencies under SR.III. |
| SR.II Criminalise terrorist financing | **PC** | • The collection of funds with the intention that they should be used/in the knowledge that they are to be used by an individual terrorist for any purpose other than terrorist purposes is not unequivocally covered;<br>• TF offence does not fully criminalise the financing of all terrorist acts required by the TF Convention in its Article 2 (1) (a) since these acts |

| | | |
|---|---|---|
| | | are not criminalised in the PC;<br>• For conducts addressed in the specific UN treaties referred to by Art. 2 of the TF Convention which are covered by Article 237, an additional purposive element is required which limits the application of TF offence;<br>• TF offence does not cover all situations where a person finances a terrorist act committed abroad. |
| SR.III Freeze and confiscate terrorist assets | **PC** | • The requirement to apply freezing measures under UNSCR 1267 and 1373 without delay is not met;<br>• There is no 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;<br>• No measures have been taken to freeze funds of persons formerly known as "EU internals";<br>• No legislative framework to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions;<br>• No clear publicly-known procedures for un-freezing in a timely manner funds and assets;<br>**Effectiveness**<br>• Lack of awareness of SR III obligations by some reporting entities;<br>• Low number of supervisory visits in relation to the implementation of international financial sanctions and no sanctions have been imposed. |
| SR.IV Suspicious transaction reporting | **LC** | • No explicit requirement to report suspicions on funds linked or related to terrorism, terrorist acts or by terrorist organisations;<br>**Effectiveness**<br>• Leaving the initial postponement decision to the reporting entity may negatively impact on the effectiveness. |

| | | |
|---|---|---|
| SR.V International co-operation[83] | **LC** | • The application of dual criminality may negatively impact Estonia's ability to provide assistance due to shortcomings identified in respect to the scope of the TF offence;<br>• Deficiencies identified under R. 3 may restrict the range of mutual legal assistance that can be provided (c.36.1(f)). |
| *SR.VI AML requirements for money/value transfer services* | ***LC*** | • Lack of effective supervision of payment service providers. |
| *SR.VII Wire transfer rules* | ***LC*** | • There is no proper monitoring of Regulation (EC) No. 1781/2006 which is aimed to cover the requirements of SR VII. |
| SR.VIII Non-profit organisations | **LC** | • Absence of effective supervision of NPOs;<br>• Limited outreach to NPOs. |
| SR.IX Cross Border declaration and disclosure | **LC** | • Low sanctions. |

[83] The review of Special Recommendation V has taken into account those Recommendations that are rated in this report. In addition it has also taken into account the findings from the 3rd round report on Recommendations 37, 38 and 39.

## TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

| AML/CFT System | Recommended Action (listed in order of priority) |
|---|---|
| **1. General** | |
| **2. Legal System and Related Institutional Measures** | |
| 2.1 Criminalisation of Money Laundering (R.1) | • Amendments to Art. 4 of the MLTFPA should be considered in order to align the physical elements of money laundering offence with Vienna and Palermo Conventions. More specifically, in relation to the acquisition, possession or use of property acquired as a result of criminal activity (…), the authorities should remove the purposive elements of concealing or disguising the illicit origin of the property with respect to use of proceeds by a self-launderer;<br>• As a signatory to the Warsaw Convention (CETS 198), Estonia should consider taking legislative measures to implement the provisions of Art. 9 paragraph 6 of the Convention. The judiciary should develop jurisprudence on money laundering as an autonomous offence and convict persons for ML where it is proved that the property originated from a predicate offence, without it being necessary to precisely establish which offence;<br>• The authorities should also conduct a review of the ML convictions achieved so far to determine whether the criminalisation of ML is being implemented effectively. In particular, this review should assist the authorities in examining the sentencing practices for ML by the courts and serve as a basis for developing a clear methodology to investigate and prosecute ML cases (with an emphasis on complex, third party and autonomous ML cases);<br>• The authorities should continue training prosecutors and judges on evidential thresholds for establishing underlying predicate criminality and confront the judiciary with more cases where it is not possible to establish precisely the underlying offence(s);<br>• The authorities should consider conducting more parallel financial investigations in relation to major cases of proceeds-generating crimes with a view to investigating possible ML, which should increase their effectiveness in detecting possible ML cases;<br>• Shortcomings in the definition of TF as a predicate offence should be amended. |

| | |
|---|---|
| 2.2 Criminalisation of Terrorist Financing (SR.II) | • The authorities are strongly encouraged at a minimum to: introduce the collection of funds with the intention that they should be used/in the knowledge that they are to be used by *an individual terrorist* for any purpose other than terrorist purposes; expressly criminalise the *indirect* provision or collection of funds with the unlawful intention that they should be used or in the knowledge that they are to be used to carry out terrorist acts, by a terrorist organisation or by an individual terrorist;<br>• Estonian authorities should consider amending the Penal Code so that the financing of all conducts referred to in Art. 2(1)(a) of the TF Convention and addressed in the specific UN terrorist conventions are criminalised, while at the same time, removing the additional purposive element provided under Art. 237 of the PC ("if committed with the purpose to force the state or an international organisation to perform an act or omission …). |
| 2.3 Confiscation, freezing and seizing of proceeds of crime (R.3) | • The authorities should ensure that:<br>o the confiscation of instrumentalities intended to be used in the commission of financing of terrorism is clearly provided for in the law;<br>o value confiscation of instrumentalities to ML, FT and other predicate crimes and value confiscation of laundered property be expressly provided for under Estonian law;<br>o confiscation applies to all property subject to confiscation, regardless of whether the owner or possessor has been identified;<br>o the confiscation of property that is derived from proceeds (i.e. income, profits or other benefits) to be explicitly provided for under the Penal Code, in order to avoid all confusion;<br>o deficiencies identified in the TF offence (see supra c.II.1) which potentially affect the scope of confiscation and provisional measures especially with regard to "legal" activities of terrorist organizations and individual terrorists, be remedied;<br>• Additionally, more efforts should be undertaken by the authorities to ensure that confiscation is used as a central tool for combating money laundering and predicate offences, through training of investigators, prosecutors and judges. It would also assist if clear policy statements on the priority of confiscation are made to prosecutors in particular by the appropriate senior officials (possibly by the Prosecutor General). |

| | |
|---|---|
| 2.4 Freezing of funds used for terrorist financing (SR.III) | • Domestic legislation should address the shortcoming under Art. 2 of Council Regulation 881/2002 as amended, which does not encompass the obligation 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 as per criterion II.2 of SRIII;<br>• The Estonian authorities should fully exploit the new mechanism enacted under Art.1(1) and (2) in conjunction with Art.7 and 8 of the ISA to take freezing measures against persons formerly known as EU internals. The authorities should also consider specifying the conditions which would need to be met to initiate a freezing action upon the request of a third State;<br>• The authorities should consider aligning the wording of Art.4 of the ISA act with criterion III.4 of SRIII, which requires that the freezing action should extend to funds or assets wholly or jointly owned or controlled, directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organizations;<br>• As concerns the obligations in respect of persons inadvertently affected by a freezing action, the ISA should specify what further actions the obliged entity must undertake and the timeline that must be respected, following the communication of the results of the verification by the FIU: when the person does not result to be a designated entity;<br>• Although the legislative framework for monitoring the obligations which stem from the ISA is sound, the authorities should ensure that such supervision, including on-site inspections, are indeed carried out;<br>• Authorities should consider enhancing the capacities of the FIU in respect of monitoring the obligations which stem from the ISA. |
| 2.5 The Financial Intelligence Unit and its functions (R.26) | • The power of the FIU to query additional information from lawyers should be formally extended beyond the mere correction of incomplete or incorrect information (art. 41(5) MLTFPA);<br>• Legal measures be taken to safeguard the confidentiality of the FIU information when querying a non-regulated person, by inserting a confidentiality provision in the law, applicable to all person required to provide additional information at the request of the FIU;<br>• The causes for the under-exploitation of the FIU reports by the LE and judiciary authorities, and of the arrears in the |

| | |
|---|---|
| | ensuing investigations be examined and addressed. |
| 2.6 Cross Border Declaration or Disclosure (SR.IX) | • The authorities should consider to have the information flow to the FIU formally regulated, particularly in respect of the timely information of suspected ML or TF;<br>• The sanction range should be reviewed;<br>• There should be particular focus, both by the ETCB and the FIU, on systematic international exchange of operational information to the foreign counterparts on cross-border cash transportations by their nationals. |
| **3. Preventive Measures – Financial Institutions** | |
| 3.1 Customer due diligence, including enhanced or reduced measures (R.5 to 8) | **Recommendation 5**<br>• The CDD requirements set out in the MLTFPA are broadly in line with the requirements under Recommendation 5. However, in order to further strengthen the CDD legal provisions, it is recommended that the authorities introduce the following express requirements within the law:<br>o A requirement to determine whether the customer is acting on behalf of another person (c.5.5.1);<br>o A clear requirement to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct CDD on such existing relationships at appropriate times (c.5.17);<br>• Additionally, the authorities should provide further guidance to financial institutions to assist them in understanding direct and indirect ownership and control of a legal person/arrangement and take measures to verify such information. (c.5.5.2 (a), (b));<br>• The authorities should clarify the following requirements in the law:<br>o The requirement to verify the identity the beneficial owner (c.5.5);<br>o The requirement to identify and verify the identity of the beneficiary under the policy (c.5.5);<br>o The requirement 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 (c.5.7.1);<br>• The authorities should also consider undertaking the following measures to improve effectiveness:<br>o Require financial institutions to request a beneficial ownership declaration signed by the beneficial owner |

| | |
|---|---|
| | in higher risk situations;<br>o A clear requirement to register information of source of funds and verify such information on the basis of documents in higher risk situations;<br>o Requiring financial institutions to include in their rules of procedure the requirement to assess the adequacy of AML/CFT systems of EEA states where the prospective customer is from or in such states;<br>o Requiring financial institutions to have procedures in place to identify equivalent third countries (FATF has in the past challenged the reliability of the EU list);<br>o Review the MLTFPA to ensure that reference to a customer, a person participating in a transaction, a person participating in a professional operation, or a person using a professional service is used consistently (especially in Art. 13(1)1));<br>• In order to improve the effective implementation of CDD requirements, the authorities should undertake further training and awareness-raising sessions with financial institutions, especially payment service providers and currency exchange operators, in particular on issues such as the identification and verification of beneficial owners, verification of source of funds and the measures to be taken when a financial institution is unable to complete the CDD procedure. |
| 3.4 Financial institution secrecy or confidentiality (R.4) | • With respect to the provisions relating to sharing of information between financial institutions where this is required by R.7, R.9 and SR VII, the Government of Estonia should simplify and clarify the language in the provisions as suggested in the 3rd round mutual evaluation report and provide further guidance to financial institutions. |
| 3.5 Record keeping and wire transfer rules (R.10 & SR.VII) | • The requirement to maintain identification data, account files, transaction data and business correspondence for at least five years following the termination of an account or a business relationship, or longer if requested by a competent authority should be regulated by law or regulation. |
| 3.6 Monitoring of transactions and relationships (R.11 & 21) | **Recommendation 11**<br>• The Government of Estonia should revisit the provisions relating to ongoing monitoring of a business relationship, to make it clear that, on discovering a complex or unusual transaction or pattern of transactions, institutions are required to investigate the background and purpose of the transaction(s) and to keep records of their findings, |

| | |
|---|---|
| | regardless of whether a notification is made to the FIU.<br><br>**Recommendation 21**<br><br>• Estonia should revisit the provisions around monitoring, to make it clear that, on discovering a transaction with no apparent economic or visible lawful purpose during monitoring of higher risk countries, institutions are required to investigate the background and purpose of the transaction(s) and keep records of their findings, regardless of whether a SAR is made;<br><br>• Estonia should revisit the provisions around monitoring, to make it clear that the obligation applies to a customer or person from one of the stipulated countries;<br><br>• Estonia should ensure that the circular letters that inform financial institutions of countries not sufficiently applying FATF Recommendations are distributed to all financial institutions, including those supervised by the FIU. |
| 3.7 Suspicious transaction reports and other reporting (R.13,14, 19, 25 & SR.IV) | • The deficiency in the TF reporting obligation of Art. 32(1) should be addressed;<br><br>• The authorities should impose the rule of the *a priori* reporting duty before executing the suspect operation and shift the postponement decision to the FIU;<br><br>• The FIU should continue to raise awareness of and provide training to the weakly or non-performing entities. |
| 3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 and 25) | **Recommendation 23**<br><br>• The authorities should consider amending the wording of Article 48(3) to ensure that supervisors have access to all records, documents or information relevant to monitoring compliance, including all documents or information related to accounts or other business relationships, or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions;<br><br>• The FSA should consider, as appropriate, undertaking more supervisory action on life insurance companies, investment firms and payment service providers;<br><br>• The Estonian authorities should also review the staffing levels at the FIU to ensure that sufficient supervisory staff are in place to effectively cover the full range of entities supervised for compliance with AML/CFT obligations, including increasing the number of on-site inspections. The FIU should introduce a proper internal methodology for supervisory purposes to ensure that on-site inspections are conducted in a systematic manner.<br><br>**Recommendation 17** |

| | |
|---|---|
| | • The Estonian Authorities should review the sanctioning provisions in the MLTFPA and the various sectoral legislation, in order to provide for consistent application of sanctions across all financial institutions;<br>• The Estonian authorities should review the range of financial penalties available, to ensure that they are sufficiently proportionate, dissuasive and effective;<br>• The Estonian authorities should extend the power to apply sanctions to directors and senior managers of financial institutions;<br>• The Estonian authorities should also use a wider range of sanctions, financial penalties and sanctions against individuals where appropriate;<br>• Sanctions imposed by the FSA and the FIU should be published, where appropriate.<br>**Recommendation 29**<br>• Estonian Authorities should consider reviewing the use of supervisory powers in the MLTFPA and the various sectoral legislation, in order to provide for consistent application of supervision across all financial institutions. In particular they should consider amending Art. 48 of MLTFPA to include the wider application of powers that is contained in the sectoral legislation;<br>• The Estonian authorities should introduce a power to apply sanctions to directors and senior managers of financial institutions. |
| **4. Preventive Measures – Non-Financial Businesses and Professions** | |
| 4.1 Customer due diligence and record-keeping (R.12) | **Applying Recommendation 5**<br>• The Estonian authorities should apply the recommendations made under Recommendations 5;<br>• The Estonian authorities should also:<br>o strengthen the awareness and effective implementation of the risk based approach (extent of CDD requirements);<br>o strengthen the awareness and effective implementation of identification and verification of source of funds, at least in high risk cases and customers;<br>o strengthen the awareness and effective implementation of beneficial owner;<br>o strengthen effective implementation of the CDD |

| | |
|---|---|
| | requirements with regard to real estate agents;<br>o strengthen effective implementation of the CDD requirements with regard to dealers in precious metals and dealers in precious stones (and high value dealers);<br>**Applying Recommendation 10**<br>• The Estonian authorities should apply the recommendations made under Recommendations 10;<br>• Estonian authorities should strengthen effective implementation of the record-keeping requirements with regard to real estate agents.<br>**Applying Recommendation 11**<br>• The Estonian authorities should apply the recommendations made under Recommendations 11. |
| 4.2 Suspicious transaction reporting (R.16) | **Applying Recommendation 13**<br>• The Estonian authorities should apply the recommendations made under Recommendations 13;<br>• The underperforming real estate sector requires closer attention and more awareness raising, if needed by applying exemplary and effective sanctions;<br>**Applying Recommendation 21**<br>• The Estonian authorities should apply the recommendations made under Recommendations 21;<br>• In addition, the FIU should consider issuing specific guidance to DNFBPs in relation to this obligation. |
| 4.3 Regulation, supervision and monitoring (R.24-25) | • The Estonian authorities should review the risk model used by the FIU to ensure that appropriate resources are applied to all subsectors, as well as to those individual entities that present higher risk of money laundering or terrorist financing;<br>• The Estonian authorities should also review the staffing levels at the FIU to ensure that sufficient supervisory staff are in place to effectively cover the full range of entities supervised for compliance with AML/CFT obligations;<br>• The Bar Association and Chamber of Notaries should review the way they formulate their supervisory programmes, to ensure that resources are applied to those institutions or members that demonstrate the higher risk of money laundering or terrorist financing. They should also review the content of the supervisory interactions, to ensure that compliance with AML/CFT obligations is given sufficient attention during the onsite inspections; |

| | |
|---|---|
| | • The Estonian authorities should review the sanctions available to the various supervisors under the MLTFPA, the Bar Association Act and the Notaries Act in order to ensure consistent application of disciplinary measure across all sectors;<br>• The FIU should also consider use of a wider range of sanctions, including public sanctions, financial penalties and sanctions against individuals where appropriate. |
| **5. Legal Persons and Arrangements & Non-Profit Organisations** | |
| 5.1 Legal persons – Access to beneficial ownership and control information (R.33) | • As suggested in the 3rd round mutual evaluation report and in the absence of any information or examples that indicate effective oversight of compliance with the obligations, the Government of Estonia should consider implementing a programme of monitoring or supervision of the full range of obligations on legal persons to hold and submit updated information to the commercial registers;<br>• Also as suggested in the 3rd round mutual evaluation report, the Government of Estonia should consider reviewing its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership and control of legal persons. |
| 5.3 Non-profit organisations (SR.VIII) | • Further outreach should be initiated towards those NPOs that are not members of NENO;<br>• Authorities should consider introducing effective supervision of NPOs and review of reports submitted by NPOs by the Court registry;<br>• Evaluators encourage authorities to conduct periodic reassessments by reviewing new information on the sector‘s potential vulnerabilities to terrorist activities. In these reassessments all relevant state authorities should be included in order to assist FIU. |
| **6. National and International Co-operation** | |
| 6.1 National co-operation and coordination (R.31 and 32) | • Although the cooperation between the relevant bodies appears to be working effectively in practice, it is recommended for all supervisory authorities to consider signing formal agreements for cooperation and coordination on supervisory matters. This should translate into more systematic national cooperation and coordination between all supervisory authorities in the AML/CFT field. |

| | |
|---|---|
| 6.2 The Conventions and UN Special Resolutions (R.35 & SR.I) | • Estonia should take necessary measures to remedy identified deficiencies under Recommendations 1 and 3 and Special Recommendation II to fully implement the Vienna, Palermo and TF Conventions;<br>• In addition, the Estonian authorities should also take steps to address the deficiencies identified under SR.III to fully implement the requirements of the UNSCRs. |
| 6.3 Mutual Legal Assistance (R.36-38 & SR.V) | • The authorities should introduce clear time limits for the evaluation and execution of MLA requests. They should also put in place a system enabling them to monitor the quality and speed of executed requests;<br>• The authorities should clarify in the law that Art. 436($1^2$) also applies to non-EU members states. |
| 6.5 Other Forms of Co-operation (R.40 & SR.V) | • The statistical data kept by the FIU should be complemented by information on the grounds for refusal or non-execution. The other relevant law enforcement authorities should start maintaining ML/FT specific statistics on operational cross-border exchanges;<br>• Supervisory authorities should maintain statistics on requests for information. |
| **7. Other Issues** | |
| 7.1 Resources and statistics (R. 30 & 32) | **Recommendation 30**<br>• The Estonian authorities should also review the staffing levels at the FIU to ensure that sufficient supervisory staff are in place to conduct supervision effectively;<br>**Recommendation 32**<br>• It is strongly recommended that the Ministry of Justice maintains additional information such as the underlying predicate offence, whether the latter was committed domestically or abroad, the sentences handed down, the amounts laundered and whether the convictions were for self-laundering, third party ML, stand-alone ML and autonomous ML. This will enable the authorities to determine, to a greater extent, whether Recommendation 1 is being implemented effectively;<br>• The ETCB should consider maintaining separate statistics on the number of cases where cash was restrained following a false declaration and where there is a suspicion of ML/FT;<br>• The FIU should maintain statistics on whether a request made by another FIU has been granted or refused;<br>• The authorities should collect statistics on formal (and |

| | |
|---|---|
| | informal) requests for assistance made or received by supervisors, including whether such requests were granted or refused;<br>• The FIU should maintain statistics on on-site inspections broken down by category of financial institution. |

## TABLE 3: AUTHORITIES' RESPONSE TO THE EVALUATION (IF NECESSARY)

| RELEVANT SECTIONS AND PARAGRAPHS | COUNTRY COMMENTS |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# V. COMPLIANCE WITH THE 3RD EU AML/CFT DIRECTIVE

Estonia has been a member country of the European Union since 2004. It has **Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing** (hereinafter: "the Directive") and the **Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis**.

The following sections describe the major differences between the Directive and the relevant FATF 40 Recommendations plus 9 Special Recommendations.

| **1.** | **Corporate Liability** |
|---|---|
| *Art. 39 of the Directive* | Member States shall ensure that natural and legal persons covered by the Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. |
| *FATF R. 2 and 17* | Criminal liability for money laundering should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply. |
| *Key elements* | The Directive provides no exception for corporate liability and extends it beyond the ML offence even to infringements which are based on national provisions adopted pursuant to the Directive. What is the position in your jurisdiction? |
| *Description and Analysis* | The corporate liability can be applied in cases mentioned in the special part of the PC.<br><br><u>*Art. 14. Liability of legal persons*</u><br><br>*(1) In the cases provided by law, a legal person shall be held responsible for an act which is committed in the interests of the legal person by its body, a member thereof, or by its senior official or competent representative.*<br>*(2) Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.*<br><br>*(3) The provisions of this Act do not apply to the state, local governments or to legal persons in public law.*<br><br>For example, the Art. 394 of the PC (money laundering) establishes that money laundering, if committed by a legal person, is punishable by a pecuniary punishment and if the legal person committed money laundering by a group, at least twice, on a large-scale basis, or by a criminal organization, the court may sentence pecuniary punishment or |

| | |
|---|---|
| | compulsory dissolution of the legal person.<br>Art. 14(1) of the PC was amended in 2008 to include all competent representatives and also to single out that any member of a body of the legal person may be held individually liable for the acts committed.<br>In recent years several legal persons have been prosecuted for ML offence.<br>2009 - 9 legal persons;<br>2010 - 4 legal persons;<br>2011 - 4 legal persons;<br>2012 - 6 legal persons.<br>The sanctioning regime has been changed in the MLTFPA. Extrajudicial proceedings concerning the misdemeanours provided for in Art. 57-64 of the MLTFPA shall be conducted by the Police and Border Guard Board and the FSA. According to these amendments all violations of the MLTFPA by both natural and legal persons are directly sanctionable. |
| *Conclusion* | Estonia has implemented Art. 39 of the Directive. |
| *Recommendations and Comments* | No recommendations. |

| **2.** | **Anonymous accounts** |
|---|---|
| *Art. 6 of the Directive* | Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. |
| *FATF R. 5* | Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. |
| *Key elements* | Both prohibit anonymous accounts but allow numbered accounts. The Directive allows accounts or passbooks on fictitious names but always subject to full CDD measures. What is the position in your jurisdiction regarding passbooks or accounts on fictitious names? |
| *Description and Analysis* | It is stated in Art. 15(3) of the MLTFPA explicitly that a credit institution and a financial institution shall not enter into a contract or make a decision on opening an anonymous account or savings bank book. A transaction in violation of the prohibition shall be void. This provision corresponds to Art. 6 of the Directive and FATF Recommendation 5.<br>It is also stated in Art. $57^3$ that decision made by an employee of a credit or financial institution to open an anonymous bank account or savings bank book, or conclusion of a relevant contract is punishable by a fine up |

| | |
|---|---|
| | to 300 fine units (1 fine unit equals 4 euros) and the same act, if committed by a legal person, is punishable by a fine up to 32,000 euros.<br>As already underlined in the 3rd round MER, the MLTFPA goes further and obliges all credit and financial institutions to offer only services that can be used only with identification of the person participating in the transaction and verification of submitted information. A credit institution and a financial institution are also obligated to open an account and keep an account only in the name of the account holder (MLTFPA Art. 15(2)). |
| *Conclusion* | MLTFPA neither allows for anonymous passbooks/accounts nor passbooks/accounts on fictitious names.<br>Estonia is in compliance with the Directive and the FATF Recommendations. |
| *Recommendations and Comments* | No recommendations. |

| **3.** | **Threshold (CDD)** |
|---|---|
| *Art. 7 b) of the Directive* | The institutions and persons covered by the Directive shall apply CDD measures when carrying out occasional transactions amounting to EUR 15,000 or more. |
| *FATF R. 5* | Financial institutions should undertake CDD measures when carrying out occasional transactions above the applicable designated threshold. |
| *Key elements* | Are transactions and linked transactions of EUR 15,000 covered? |
| *Description and Analysis* | Article 12(2)2) of the MLTFPA requires CDD measures to be undertaken when carrying out occasional transactions amounting to 15,000 euros or more, regardless whether the financial obligation is performed in one payment or in several related payments. CDD have to be carried out as soon as the exceeding of the amount provided for in Art. 12(2)2) becomes evident.<br>The threshold is equal to that of the Directive. This provision is applicable to all obligated persons. |
| *Conclusion* | Transactions and linked transactions of EUR 15,000 are covered. |
| *Recommendations and Comments* | No recommendations. |

| 4. | Beneficial Owner |
|---|---|
| *Art. 3(6) of the Directive (see Annex)* | The definition of 'Beneficial Owner' establishes minimum criteria (percentage shareholding) where a natural person is to be considered as beneficial owner both in the case of legal persons and in the case of legal arrangements. |
| *FATF R. 5 (Glossary)* | 'Beneficial Owner' refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or legal arrangement. |
| *Key elements* | Which approach does your country follow in its definition of "beneficial owner"? Please specify whether the criteria in the EU definition of "beneficial owner" are covered in your legislation. |
| *Description and Analysis* | Article 8 of the MLTFPA determines the provisions of beneficial owner which is in line with Art. 3(6) of the Directive but also refers to the FATF definition.<br>***Article 8. Beneficial owner***<br>*(1) A beneficial owner is a natural person who, taking advantage of their influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed.*<br>*($1^1$) A beneficial owner is also a natural person who ultimately holds the shares or voting rights in a company or exercises final control over management of a company in at least one of the following ways:*<br>*1) by holding over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;*<br>*2) otherwise exercising control over management of a legal person.*<br>*(2) A beneficial owner is also a natural person who, to the extent of no less than 25 percent determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, or who exercises control over the property of a legal person, civil law partnership or another contractual legal arrangement to the extent of no less than 25 percent.*<br>*(3) A beneficial owner is also a natural person who, to an extent not determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, and primarily in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates.*<br>*(4) Clause 1) of subsection ($1^1$) of this section does not apply to companies whose securities have been listed on a regulated stock* |

| | |
|---|---|
| | *exchange.* |
| *Conclusion* | Estonia is in compliance with the Directive, but also refers to the FATF definition (person on whose behalf a transaction is conducted.) |
| *Recommendations and Comments* | No recommendations. |

| **5.** | **Financial activity on occasional or very limited basis** |
|---|---|
| *Art. 2 (2) of the Directive* | Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or financing of terrorism occurring do not fall within the scope of Art. 3(1) or (2) of the Directive.<br>Art. 4 of Commission Directive 2006/70/EC further defines this provision. |
| *FATF R. concerning financial institutions* | When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially (2004 AML/CFT Methodology para 23; Glossary to the FATF 40 plus 9 Special Recs.). |
| *Key elements* | Does your country implement Art. 4 of Commission Directive 2006/70/EC? |
| *Description and Analysis* | Estonia has decided not make use of the option to implement Art. 2(2) of the Directive rendering Art. 4 of the Directive 2006/70/EC not applicable. |
| *Conclusion* | Estonia has decided not to implement Art. 4 of Commissions Directive2006/70/EC. |
| *Recommendations and Comments* | No recommendations. |

| **6.** | **Simplified Customer Due Diligence (CDD)** |
|---|---|
| *Art. 11 of the Directive* | By way of derogation from the relevant Art. the Directive establishes instances where institutions and persons may not apply CDD measures. However the obligation to gather sufficient CDD information remains. |

| | |
|---|---|
| *FATF R. 5* | Although the general rule is that customers should be subject to the full range of CDD measures, there are instances where reduced or simplified measures can be applied. |
| *Key elements* | Is there any implementation and application of Art. 3 of Commission Directive 2006/70/EC which goes beyond the AML/CFT Methodology 2004 criterion 5.9? |
| *Description and Analysis* | Article 17 of the MLTFPA defines the application of simplified CDD measures, which can be applied if the conditions in Art. 18 of the MLTFPA are met. An obligated person may, in the event of low risk, take CDD measures specified in Art. 13(1) of the MLTFPA pursuant to a simplified procedure, determining the scope based on the nature of the business relationship or the risk level of the transaction. Simplified CDD is allowed in the cases (certain person, customer or transaction) determined in the Art. 18 of the MFTFPA.<br><br>Article 17(3) requires obligated persons to gather enough information to determine whether the customer or transactions qualifies for simplified CDD.<br><br>The conditions and cases (certain person, customer or transaction) determined in the Art. 18 of the MFTFPA reflects and are in line with the requirements of Art. 3 of the Commission Directive 2006/70/EC with the exception of the requirement of non-anonymity, which follows from Art. 15(2) of the MLTFPA. CDD must be applied but in a simplified procedure.<br><br>Article 18(5) of the MLTFPA authorizes the Ministry of Finance to enact a regulation which establishes further criteria for low risk and the regulation of the Minister of Finance of Estonia No 11 of 3 April 2008 does so, going also beyond the criterion 5.9 of the AML/CFT Methodology 2004.<br><br>Estonia leaves it to the financial institutions to apply simplified CDD measures vis-a-vis any person, based on the risk-based-approach. Pursuant to the Art. 5 of the Directive, Estonia has chosen not to list mandatory subjects to the simplified CDD in the law, leaving it to the discretion of obligated persons. |
| *Conclusion* | Article 17 of the MLTFPA is in line with Directives 2005/60/EC and 2006/70/EC. |
| *Recommendations and Comments* | No recommendations. |

| **7.** | **Politically Exposed Persons (PEPs)** |
|---|---|
| *Art. 3 (8), 13 (4) of the* | The Directive defines PEPs broadly in line with FATF 40 (Art. 3(8)). |

| | |
|---|---|
| *Directive*<br>*(see Annex)* | It applies enhanced CDD to PEPs residing in another Member State or third country (Art. 13(4)). Directive 2006/70/EC provides a wider definition of PEPs (Art. 2) and removal of PEPs after one year of the PEP ceasing to be entrusted with prominent public functions (Art. 2(4)). |
| *FATF R. 6 and Glossary* | Definition similar to Directive but applies to individuals entrusted with prominent public functions in a foreign country. |
| *Key elements* | Does your country implement Art. 2 of Commission Directive 2006/70/EC, in particular Art. 2(4), and does it apply Art. 13(4) of the Directive? |
| *Description and Analysis* | Politically Exposed Persons are defined in Art. 20(1) of the MLTFPA.<br>*A politically exposed person is a natural person who performs or has performed prominent public functions, their family members and close associates. A person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, and the family members or close associates of such person are not considered politically exposed persons.*<br><br>According to Art. 21 of the MLTFPA the transactions involving the participation of a politically exposed person are subject to enhanced due diligence by the obligated person (in line with 13(4) of the Directive). |
| *Conclusion* | Estonia is in compliance with the Directive. Art. 2(4) of Commission Directive have been implemented. Art. 13(4) of Directive is fully implemented. |
| *Recommendations and Comments* | No recommendations. |

| **8.** | **Correspondent banking** |
|---|---|
| *Art. 13 (3) of the Directive* | For correspondent banking, Art. 13(3) limits the application of Enhanced Customer Due Diligence (ECDD) to correspondent banking relationships with institutions from non-EU member countries. |
| *FATF R. 7* | Recommendation 7 includes all jurisdictions. |
| *Key elements* | Does your country apply Art. 13(3) of the Directive? |
| *Description and Analysis* | Article 22 of the MLTFPA regulates correspondent banking relationships. It was suggested in the 3rd round MER that Estonia should ensure better compliance with the Directive and amend the law |

| | |
|---|---|
| | to include a requirement to acquire senior management approval for the establishment of correspondent banking relationships and ensure that the responsibilities of the correspondent parties regarding AML/CFT duties are fully laid out in the correspondent banking arrangements. Estonia prepared the relevant changes to the MLTFPA in 2009 and the amended Art. 22 of the MLTFPA reads as follows.<br><br>***Article 22. Correspondent relationships of credit and financial institutions***<br><br>*(1) A credit institution and a financial institution shall take enhanced due diligence measures upon opening a correspondent account with a credit institution of a third country and during the period of validity of the respective contract, thereby regularly assessing the following:*<br><br>*1) based on public information, the nature of the economic activities and the trustworthiness and reputation of the credit institution of the third country and the effectiveness of supervision exercised over the credit institution;*<br><br>*2) the control systems of the credit institution of the third country for prevention of money laundering and terrorist financing.*(emphasis added)<br><br>*(2) The contract serving as the basis for opening a correspondent account or the rules of procedure of the credit institution shall contain the prohibition to open a correspondent account for a credit institution which corresponds to the condition specified in clause (3) 1), and the obligations of the parties:*<br><br>*1) upon application of due diligence measures for prevention of money laundering and terrorist financing, including with regard to a customer having access to a payable-through account or another similar account;*<br><br>*2) upon submission, on the basis of a query, of data gathered in the course of identification of customers and verification of submitted information;*<br><br>*3) upon preservation of data and upon performance of the notification obligation and application of other measures for prevention of money laundering and terrorist financing.*<br><br>*($2^1$) Prior consent of the management board of the credit institution or financial institution or the person authorised by the management board is required for opening a correspondent account for a credit institution or a financial institution of a third country or for opening a correspondent account in a third country credit institution or financial institution or for signing the corresponding contract.*(emphasis added)<br><br>*(3) Credit institutions and financial institutions are prohibited to open or hold a correspondent account in a credit institution, which meets at least one of the following conditions:*<br><br>*1) the actual place of management or business of the credit institution is located outside its country of location and the credit* |

| | |
|---|---|
| | *institution is not part of the consolidation group or group of undertakings of a credit institution or financial institution that is subject to sufficient supervision;*<br><br>*2) an account for a credit institution corresponding to the characteristics specified in clause 1) has been opened in the credit institution;*<br><br>*3) according to international standards or the circumstances provided for in this section, which are to be used as a basis for assessment, deficiencies become evident in the trustworthiness of the executives of the credit institution and in assessment of measures for prevention of money laundering and terrorist financing.*<br><br>*(4) An agreement in violation of the prohibition of opening a correspondent account in a credit institution corresponding to the conditions specified in clauses (3) 1) and 2) shall be void.*<br><br>*(5) Subsections (3) and (4) shall be applied to correspondent relationships with institutions and undertakings whose principal and permanent activity lies in entering into transactions resembling those provided for in subsection 6 (1) of the Credit Institutions Act.*<br><br>The amendments entered into force on 26th December 2009. |
| *Conclusion* | Estonia applies Art. 13 (3) of the Directive. |
| *Recommendations and Comments* | No recommendations. |

| **9.** | **Enhanced Customer Due Diligence (ECDD) and anonymity** |
|---|---|
| *Art. 13 (6) of the Directive* | The Directive requires ECDD in case of ML or TF threats that may arise from products or transactions that might favour anonymity. |
| *FATF R. 8* | Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity [...]. |
| *Key elements* | The scope of Art. 13(6) of the Directive is broader than that of FATF R. 8, because the Directive focuses on products or transactions regardless of the use of technology. How are these issues covered in your legislation? |
| *Description and Analysis* | The Art. 13(6) has been transposed to the Estonian legislation with the MLTFPA Art. 30(3)2), which establishes that all obligated persons should have rules of procedure in place, that describe, *transactions of a higher risk level, including risks arising from means of communication, computer network and other technological development, and establish the appropriate requirements and procedure for entering into and monitoring such transactions.* |

| | |
|---|---|
| | This section was amended after the 3rd round MER was adopted by the plenary of MONEYVAL and entered into force on 26th December 2009.<br>Apart from this specific provision, the Art. 15(2) of the MLTFPA is in force, forbidding credit and financial institutions to provide services which can be used without prior identification and verification of the customer. |
| *Conclusion* | Estonia implemented Art. 13(6) of the Directive. |
| *Recommendations and Comments* | No recommendations. |

| **10.** | **Third Party Reliance** |
|---|---|
| *Art. 15 of the Directive* | The Directive permits reliance on professional, qualified third parties from EU Member States or third countries for the performance of CDD, under certain conditions. |
| *FATF R. 9* | Allows reliance for CDD performance by third parties but does not specify particular obliged entities and professions which can qualify as third parties. |
| *Key elements* | What are the rules and procedures for reliance on third parties? Are there special conditions or categories of persons who can qualify as third parties? |
| *Description and Analysis* | According to Art. 14(4) of the MLTFPA Estonian obligated persons are allowed to rely on "*information received by the obligated person in a format that can be reproduced in writing from a credit institution registered in the Estonian commercial register or from a branch of a foreign credit institution or from a credit institution that has been registered or whose place of business is in a contracting state of the European Economic Area or a third country where requirements equal to those provided in this Act are in force*."<br><br>The MLTFPA Art. 6(1)2) provides that credit institutions in the MLTFPA are to be defined within the meaning of the CrIA and, additionally, branches of foreign credit institutions registered in the Estonian commercial register. |
| *Conclusion* | It can be concluded that Estonia's approach is considerably more restrictive than allowed for the Directive (Art. 15) and Estonia is in compliance with the Directive. |
| *Recommendations and Comments* | No recommendations. |

| 11. | Auditors, accountants and tax advisors |
|---|---|
| *Art. 2 (1)(3)(a) of the Directive* | CDD and record keeping obligations are applicable to auditors, external accountants and tax advisors acting in the exercise of their professional activities. |
| *FATF R. 12* | CDD and record keeping obligations<br>1. do not apply to auditors and tax advisors;<br>2. apply to accountants when they prepare for or carry out transactions for their client concerning the following activities:<br>• buying and selling of real estate;<br>• managing of client money, securities or other assets;<br>• management of bank, savings or securities accounts;<br>• organisation of contributions for the creation, operation or management of companies;<br>• creation, operation or management of legal persons or arrangements, and buying and selling of business entities (2004 AML/CFT Methodology criterion 12.1(d)). |
| *Key elements* | The scope of the Directive is wider than that of the FATF standards but does not necessarily cover all the activities of accountants as described by criterion 12.1(d). Please explain the extent of the scope of CDD and reporting obligations for auditors, external accountants and tax advisors. |
| *Description and Analysis* | Article 3(1) of the MLTFPA imposes the Act to apply to the economic or professional activities of<br>• auditors and providers of accounting services;<br>• providers of accounting or tax advice services;<br>These types of service providers are obligated persons (MLTFPA Art. 10), the obligations raising from the MLTFPA to the obligated persons are also mandatory to auditors, providers of accounting services and providers of accounting or tax advice services. That includes all the provisions covering CDD and record keeping. It was concluded in the 3rd round MER that no exemptions to maintenance and preservation of records were made regarding auditors, tax advisors and accountants and no recommendations were made in the 3rd round MER. |
| *Conclusion* | MLTFPA does not make any exemptions to apply CDD measures or to maintenance and preservation of records for auditors, tax advisors and accountants who are required to fulfill the the obligations as financial institutions. |
| *Recommendations and Comments* | No recommendations. |

| 12. | High Value Dealers |
|---|---|
| *Art. 2(1)(3)e) of the Directive* | The Directive applies to natural and legal persons trading in goods where payments are made in cash in an amount of EUR 15,000 or more. |
| *FATF R. 12* | The application is limited to those dealing in precious metals and precious stones. |
| *Key elements* | The scope of the Directive is broader. Is the broader approach adopted in your jurisdiction? |
| *Description and Analysis* | The approach taken in Estonia and implemented in the MLTFPA is broader than the Directive would require. The MLTFPA has brought under its scope all traders in goods: "*traders for the purposes of the Trading Act, if a cash payment of more than 15,000 euros or an equal amount in another currency is made to the trader, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments*".<br><br>Additionally, the persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones are brought under the scope (without any threshold for payments). Exempt are these persons that trade in precious metals and precious metal articles used for production, scientific or medical purposes.<br><br>The term "trader" in the Trading Act means a person or body which, within the framework of the economic or professional activities thereof, offers and sells goods or offers and provides services. Hence, the traders in services are also covered. |
| *Conclusion* | The MLTFPA is in compliance with the Directive. |
| *Recommendations and Comments* | No recommendations. |

| 13. | Casinos |
|---|---|
| *Art. 10 of the Directive* | Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2,000 or more. This is not required if they are identified at entry. |
| *FATF R. 16* | The identity of a customer has to be established and verified when he or she engages in financial transactions equal to or above EUR 3,000. |

| | |
|---|---|
| *Key elements* | In what situations do customers of casinos have to be identified? What is the applicable transaction threshold in your jurisdiction for identification of financial transactions by casino customers? |
| *Description and Analysis* | The legislation of Estonia is as regards casinos (and organisers of games of chance) stricter than the Directive requires.<br><br>Article 37 of the Gambling Act provides that the organiser of a game of chance shall identify the persons entering the gaming location for games of chance.<br><br>*The following data shall be registered upon identification:*<br><br>*1) forename and surname;*<br>*2) personal identification code or date of birth in the absence of a personal identification code;*<br>*3) the name, serial number, date and place of issue of the identification document;*<br>*4) the time and date of arrival in the gaming location for games of chance.*<br><br>*A person intending to enter a gaming location for games of chance shall present an identification document for registration of the data. A copy shall be made of the page of the identification document containing personal data and entered in an electronically maintained database. Before a person enters a gaming location for games of chance, the organiser of the games of chance shall verify the data in the electronically maintained database regarding the persons who have visited the gaming location for games of chance on the basis of the identification document presented for identification and shall register the time and date of the person's arrival in the gaming location for games of chance in the database. The data of visitors of gaming location can be examined, extracts can be received and enquiries can be made about the data using a system for exchange of data based on the data security measures and computer network agreed with the organiser of the game of chance only by:*<br>*1) a supervisory authority upon exercising state supervision;*<br>*2) a court in a judicial proceeding;*<br>*3) an authority conducting preliminary investigation in a criminal matter;*<br>*4) the Tax and Customs Board in relation to the conduction of proceedings in a tax matter;*<br>*5) the Financial Intelligence Unit (*emphasis added*);*<br>*6) a security authority for performing the functions provided for in the Security Authorities Act;*<br>*7) the person himself or herself with regard to the data relating to him or her.*<br><br>Database entries regarding a person shall be stored for at least five years after the person's last visit to the gaming location for games of chance. |

| | |
|---|---|
| | Additional measures are provided in Art. 16 the MLTFPA, regarding all gaming location visitors who pay or receive in a single transaction or several related transactions an amount exceeding 2,000 euros or an equal amount in another currency. The organisers of games of chance are required to identify and verify the residential address, profession or area of activity and information on PEP status regarding all the persons who pay or recieve in a single or several related transactions an amount exceeding 2,000 euros or the equivalent amount in another currency. The Art. 23 of th MLTFPA act requires obligated entitites to identify natural persons by means of documents specified in the Identity Documents Act or a valid travel document or a driving licence. |
| *Conclusion* | The regulation of casinos in the MLTFPA is in compliance with the Directive. |
| *Recommendations and Comments* | No recommendations. |

| **14.** | **Reporting by accountants, auditors, tax advisors, notaries and other independent legal professionals via a self-regulatory body to the FIU** |
|---|---|
| *Art. 23 (1) of the Directive* | This article provides an option for accountants, auditors and tax advisors, and for notaries and other independent legal professionals to report through a self-regulatory body, which shall forward STRs to the FIU promptly and unfiltered. |
| *FATF Recommendations* | The FATF Recommendations do not provide for such an option. |
| *Key elements* | Does the country make use of the option as provided for by Art. 23 (1) of the Directive? |
| *Description and Analysis* | Estonia has not made use of the option in Art. 23(1) of the Directive. The Art. 32 of the MLTFPA requires all obligated persons to report directly to the FIU. |
| *Conclusion* | Estonia has not made use of the option in Art. 23(1) of the Directive. The Art. 32 of the MLTFPA requires all obligated persons to report directly to the FIU. |
| *Recommendations and Comments* | No recommendations. |

| 15. | Reporting obligations |
|---|---|
| *Arts. 22 and 24 of the Directive* | The Directive requires reporting where an institution knows, suspects, or has reasonable grounds to suspect money laundering or terrorist financing (Art. 22). Obliged persons should refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing and to report it to the FIU, which can stop the transaction. If to refrain is impossible or could frustrate an investigation, obliged persons are required to report to the FIU immediately afterwards (Art. 24). |
| *FATF R. 13* | Imposes a reporting obligation where there is suspicion that funds are the proceeds of a criminal activity or related to terrorist financing. |
| *Key elements* | What triggers a reporting obligation? Does the legal framework address *ex ante* reporting (Art. 24 of the Directive)? |
| *Description and Analysis* | Article 32(1) of the MLTFPA defines the reporting obligation: "*if, upon performance of economic or professional activities or professional operations or provision of professional services, an obligated person identifies an activity or circumstances which might be an indication of money laundering or terrorist financing or an attempt thereof or in the event of which the obligated person has reason to suspect or knows that it is money laundering or terrorist financing, the obligated person shall immediately, but not later than within two working days from identifying the act or circumstances or from the rise of the suspicion, notify the Financial Intelligence Unit thereof*."<br><br>Under Art. 32(5) of the MLTFPA the obligated person has the right to postpone a suspicious trasanction. The obligated person therefore has discretion in deciding whether a transaction is to be carried out or otherwise. |
| *Conclusion* | While the Directive requires financial institutions to refrain from carrying out a suspicious transaction, the MLTFPA leaves some room for discretion upon the obligated person. The MLTFPA is therefore not entirely in line with the Directive. |
| *Recommendations and Comments* | To fully implement Art. 24 of the Directive, Estonia should require obligated persons to refrain from carry out all suspicious transactions. |

| 16. | Tipping off (1) |
|---|---|
| *Art. 27 of the Directive* | Art. 27 provides for an obligation for Member States to protect employees of reporting institutions from being exposed to threats or hostile actions. |

| | |
|---|---|
| *FATF R. 14* | No corresponding requirement (directors, officers and employees shall be protected by legal provisions from criminal and civil liability for "tipping off", which is reflected in Art. 26 of the Directive) |
| *Key elements* | Is Art. 27 of the Directive implemented in your jurisdiction? |
| *Description and Analysis* | Article 35 of the MLTFPA provides a comprehensive protection of financial institutions, their directors, officers and employees concerning civil and criminal liabilitybecause of breach of any restrictions on disclosure of information. However this covers only ythe requirements of FATF Rec.14 and Art. 26 of the Directive. Art. 27 of the Directive goes beyond as it provides for an obligation for Member States to protect employees of reporting institutions and person from being exposed to threats or hostile action.<br><br>Article 43 of the MLTFPA establish restrictions on use of information. Under subsection (5), the FIU shall not in any event provide information about the obligated person who submitted information for the purpose of fulfilment of the notification obligation or the members of the directing body or employees of the person.<br><br>MLTFPA Article 43. Restrictions on the use of information<br><br>(*5) The Financial Intelligence Unit shall not disclose personal data of the person performing the notification obligation or a member or employee of the directing body of the obligated person.*<br><br>The combination of rules where on one hand there is an obligation to report to the FIU any suspicious activities and the infringement of this obligation is punishable under Art. 59, 60 and 61 and on the other hand there are strict provisions to the Financial Intelligent Unit and its employees to protect the data. According to the Estonian Authorities it is considered to be sufficient to protect persons from threats and hostility. |
| *Conclusion* | Estonia has implemented Art. 27 of the Directive. |
| *Recommendations and Comments* | No recommendations for Estonia. |

| **17.** | **Tipping off (2)** |
|---|---|
| *Art. 28 of the Directive* | The prohibition on tipping off is extended to where a money laundering or terrorist financing investigation is being or may be carried out. The Directive lays down instances where the prohibition is lifted. |
| *FATF R. 14* | The obligation under R. 14 covers the fact that an STR or related information is reported or provided to the FIU. |

| *Key elements* | Under what circumstances are the tipping off obligations applied?<br>Are there exceptions? |
|---|---|
| *Description and Analysis* | Article 34 of the MLTFPA establish the confidentiality requirement of persons with a notification obligation. According to subsection (1) "*an obligated person, and a structural unit, a member of a directing body and an employee of an obligated person who is a legal person is prohibited to notify a person, the beneficial owner or representative of the person about a notification given to the Financial Intelligence Unit about the person and about precepts made by the Financial Intelligence Unit under Art. 40 or 41 or initiation of criminal proceedings*".<br><br>An obligated person may notify a person that the Financial Intelligence Unit has restricted the use of the person's account or that other restrictions have been imposed by the unit after fulfilment of the respective precept.<br><br>On the basis of subsection (2) of Art. 34 of the MLTFPA the aforementioned rule is applied with regard to provision of information to third parties, unless otherwise provided in this Act.<br><br>Subsection (3) Art. 34 of the MLTFPA contain derogations which are in compliance with Art. 28 of the Directive. The list of persons whom information may be given, as set out in the clauses of subsection (3), is exhaustive. It must be taken into account that exchange of information is not permitted between all obligated persons and according to Recital 33 of the Directive, personal data protection legislation must be taken into account upon disclosure of information. In general it is prohibited to disclose information to third parties without the consent of the data subject.<br><br>An obligated person is allowed to disclose information within the consolidation group or financial conglomerate, provided that the same persons are subject to the obligation of professional secrecy (clause 1). Information may be exchanged only between obligated persons if the information about the specific transaction suspected, with good reason, of money laundering or terrorist financing concerns various obligated persons who operate in the same branch of the economy or profession. The prohibition of forwarding information is not applicable in the case where notaries public, attorneys or auditors act in the same legal entity (e.g. in the same law firm) or cooperation network (e.g. a network of law firms), which has the same owners, directing bodies and internal control system (clause 2).<br><br>An obligated person may give information concerning the same person and the same transaction involving two or more institutions and persons located in an EEA country or a third country, in the same professional category or branch where equivalent obligations for keeping professional secrets and protecting personal data apply (clause 3).<br><br>According to subsection (5), the prohibition of disclosure is not applied if a notary public, attorney or auditor tries to convince the client to refrain from illegal acts. |

| | |
|---|---|
| *Conclusion* | Estonia has fully implemented Art. 28 of the Directive. |
| *Recommendations and Comments* | No recommendations. |

| **18.** | **Branches and subsidiaries (1)** |
|---|---|
| *Art. 34 (2) of the Directive* | The Directive requires credit and financial institutions to communicate the relevant internal policies and procedures where applicable on CDD, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication to branches and majority owned subsidiaries in third (non EU) countries. |
| *FATF R. 15 and 22* | The obligations under the FATF 40 require a broader and higher standard but do not provide for the obligations contemplated by Art. 34(2) of the EU Directive. |
| *Key elements* | Is there an obligation as provided for by Art. 34(2) of the Directive? |
| *Description and Analysis* | Article 13(2) of the MLTFPA requires from credit and financial institutions to apply the due diligence measures in an agency, branch a subsidiary where they have a majority shareholding located in a third country and follow the requirements for collection and storage of data which are at least equal to the provisions of the MLTFPA. In the 3rd round MER of MONEYVAL it was suggested that it might be desirable to clarify the term "third countries", whereas the provisions of the MLTFPA were found to be in compliance with the Directive.<br>The CrIA provides the general definition of third countries, referring to a third country as "*a country which is not a contracting state"* and to the term "contracting state" as "*states which are contracting parties to the EEA agreement*". |
| *Conclusion* | The MLTFPA is in compliance with the Directive (Art. 34(2)). |
| *Recommendations and Comments* | No recommendations. |

| **19.** | **Branches and subsidiaries (2)** |
|---|---|
| *Art. 31(3) of the Directive* | The Directive requires that where legislation of a third country does not permit the application of equivalent AML/CFT measures, credit and financial institutions should take additional measures to effectively handle the risk of money laundering and terrorist financing. |

| | |
|---|---|
| *FATF R. 22 and 21* | Requires financial institutions to inform their competent authorities in such circumstances. |
| *Key elements* | What, if any, additional measures are your financial institutions obliged to take in circumstances where the legislation of a third country does not permit the application of equivalent AML/CFT measures by foreign branches of your financial institutions? |
| *Description and Analysis* | Second sentence of the Art. 13(2) of the MLTFPA provides that in the case of legislation of a third country not permitting the application of equivalent due diligence and record keeping measures, the credit or financial institution is obliged to immediately notify the competent supervisory authority and apply additional measures for preventing money laundering or terrorist financing risks. |
| *Conclusion* | Estonia is in compliance with the EU Directive. |
| *Recommendations and Comments* | No recommendations. |

| **20.** | **Supervisory Bodies** |
|---|---|
| *Art. 25 (1) of the Directive* | The Directive imposes an obligation on supervisory bodies to inform the FIU where, in the course of their work, they encounter facts that could contribute evidence of money laundering or terrorist financing. |
| *FATF R.* | No corresponding obligation. |
| *Key elements* | Is Art. 25(1) of the Directive implemented in your jurisdiction? |
| *Description and Analysis* | The Art. 49 of the MLTFPA establishes that *"if upon exercising supervision the Financial Supervision Authority, the board of the Bar Association, the Ministry of Justice or the Chamber of Notaries detect a situation the elements of which give rise to justified suspicion of money laundering or terrorist financing, they shall immediately notify the Financial Intelligence Unit thereof pursuant to the procedure provided in subsection 33 (4).* |
| *Conclusion* | Estonia is in compliance with the EU Directive. |
| *Recommendations and Comments* | No recommendations. |

| 20. | Systems to respond to competent authorities |
|---|---|
| *Art. 32 of the Directive* | The Directive requires credit and financial institutions to have systems in place that enable them to respond fully and promptly to enquires from the FIU or other authorities as to whether they maintain, or whether during the previous five years they have maintained, a business relationship with a specified natural or legal person. |
| *FATF R.* | There is no explicit corresponding requirement but such a requirement can be broadly inferred from Recommendations 23 and 26 to 32. |
| *Key elements* | Are credit and financial institutions required to have such systems in place and effectively applied? |
| *Description and Analysis* | According to MLTFPA Art. 26 the credit and financial institutions are required to "*preserve the original counterparts or copies of the documents specified in Art. 23 and 24, which serve as the basis for identification and verification of a person, and of the documents serving as the basis for establishment of a business relationship, for no less than five years after termination of the business relationship.*" Article 26 (3) additionally states that "*an obligated person shall preserve the documents and data specified in sections (1) and (2) in a manner which allows for a full and immediate reply to enquiries received from the Financial Intelligence Unit or, pursuant to legislation, from other investigative bodies or a court*." The obligations stipulated by Art. 26 MLTFPA (particularly the language that data have to be preserved "in a manner which allows for an exhaustive and immediate reply to enquiries from the FIU or other investigative bodies") serves as a legal basis that credit and financial institutions can fully and promptly respond to enquiries from the FIU in the circumstances described by Art. 32 of the Directive. |
| *Conclusion* | Estonia is in compliance with the Directive. |
| *Recommendations and Comments* | No recommendations. |

| 21. | Extension to other professions and undertakings |
|---|---|
| *Art. 4 of the Directive* | The Directive imposes a *mandatory* obligation on Member States to extend its provisions to other professionals and categories of undertakings other than those referred to in A.2(1) of the Directive, which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes. |
| *FATF R. 20* | Requires countries only to consider such extensions. |
| *Key elements* | Has your country implemented the mandatory requirement in Art. 4 of |

| | |
|---|---|
| | the Directive to extend AML/CFT obligations to other professionals and categories of undertaking which are likely to be used for money laundering or terrorist financing purposes? Has a risk assessment been undertaken in this regard? |
| *Description and Analysis* | Article 3 of the MLTFPA lists the persons who are required to apply preventive measures against money laundering and terrorist financing in the course of their economic and professional activities. The said list includes all institutions and persons covered in Art. 2(1) of the Directive as well as pawnbrokers. It was decided on the potential risk of money laundering and terrorist financing and based on the experience of supervisory bodies.<br><br>In 2012 two categories of obliged persons were also added: persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones and non-profit associations and foundations, if a cash payment of more than 15,000 euros or an equal amount in another currency is made to them. The inclusion was made pursuant to the risk assessment made by FIU which is also covered in Explanatory Memorandum to Draft Act to Amend the MLTFPA, the ISA and the Estonian Central Register of Securities Act. |
| *Conclusion* | The mandatory requirement in Art. 4 of the Directive has been implemented. The inclusion of other professions and categories was made pursuant to the risk assessment made by FIU. |
| *Recommendations and Comments* | No recommendations. |

| **22.** | **Specific provisions concerning equivalent third countries?** |
|---|---|
| *Art. 11, 16(1)(b), 28(4),(5) of the Directive* | The Directive provides specific provisions concerning countries which impose requirements equivalent to those laid down in the Directive (e.g. simplified CDD). |
| *FATF R.* | There is no explicit corresponding provision in the FATF 40 plus 9 Recommendations. |
| *Key elements* | How, if at all, does your country address the issue of equivalent third countries? |
| *Description and Analysis* | The list of equivalent third countries was agreed between Member States and was dealt by the European Commission working group, who has enacted a list of equivalent third countries to all member states. The list is available on-line:<br><br>http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf |

| | |
|---|---|
| | The list is published on the web-sites of both FIU and FSA.<br>http://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/riigid-kus-kehtivad-rahapesu-ja-terrorismi-rahastamise-samavaarsed-nouded.dot<br>http://www.fi.ee/public/aml/AML_3rd_equiv_comm_underst_est.pdf |
| *Conclusion* | The MLTFPA contains reference on third countries having equal requirements to those provided in the Act. The list of the equivalent third countries is published on the website of the FIU and FSA. The provisions in the MLTFPA on equivalent third countries correspond to the requirements of the Directive. |
| *Recommendations and Comments* | No recommendations. |

**Annex to Compliance with 3rd EU AML/CFT Directive Questionnaire**

**Article 3 (6) of EU AML/CFT Directive 2005/60/EC (3rd Directive):**

(6) "beneficial owner" means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;

(ii) the natural person(s) who otherwise exercises control over the management of a legal entity:

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;

(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;

**Article 3 (8) of the EU AML/CFT Directive 2005/60EC (3rd Directive):**

(8) "politically exposed persons" means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;

**Article 2 of Commission Directive 2006/70/EC (Implementation Directive):**

Article 2

Politically exposed persons

1. For the purposes of Article 3(8) of Directive 2005/60/EC, "natural persons who are or have been entrusted with prominent public functions" shall include the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliaments;

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(d) members of courts of auditors or of the boards of central banks;

(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(f) members of the administrative, management or supervisory bodies of State-owned enterprises.

None of the categories set out in points (a) to (f) of the first subparagraph shall be understood as covering middle ranking or more junior officials.

The categories set out in points (a) to (e) of the first subparagraph shall, where applicable, include positions at Community and international level.

2. For the purposes of Article 3(8) of Directive 2005/60/EC, "immediate family members" shall include the following:

(a) the spouse;

(b) any partner considered by national law as equivalent to the spouse;

(c) the children and their spouses or partners;

(d) the parents.

3. For the purposes of Article 3(8) of Directive 2005/60/EC, "persons known to be close associates" shall include the following:

(a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in paragraph 1;

(b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 1.

4. Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of paragraph 1 of this Article for a period of at least one year, institutions and persons referred to in Article 2(1) of Directive 2005/60/EC shall not be obliged to consider such a person as politically exposed.

# VI. LIST OF ANNEXES

Please see document MONEYVAL(2014)20_ANN.